Active Network Probing Framework for Real-Time Detection of Anomalous Internet Traffic Patterns

P. Kharabi[1]*, El Fanaa Jarhoumi[2]

[1, 2]College of Applied Science, University of Technology and Applied Sciences, Ibri, Sultanate of Oman

Keywords:
Active probing,
Aanomaly detection,
Internet traffic,
Network measurement,
DDoS detection,
Real-time monitoring,
Traffic analytics

Author's Email id:
kharbi.p@gmail.com,
el.fanaa.jar@gmail.com

DOI: 10.31838/IJCCTS.13.02.08

Received : 09.04.25

Revised : 11.06.25

Accepted : 13.08.25

Abstract

The growing size and sophistication of the worldwide Internet systems require effective techniques of real-time monitoring of abnormal network activity. The given paper presents an active network probing framework which repeatedly measures the quality of end-to-end Internet paths with lightweight ICMP and TCP-based measurement packets. The framework is dynamically tweaked to either shorten or lengthen its probing interval, based on the volatility of the network that it monitors, allowing it to distinguish between a benign congestion event and an anomaly caused by an attack, e.g. by Distributed Denial-of-Service (DDoS) amplification or route hijacking. The probes are spread on ten geographically different vantage points that offer coverage and a high level of temporal granularity. Information regarding the collected data is analysed with a hybrid statistical-machine learning model that matches traffic deviations on real-time. Experimental tests had 92% accuracy in anomaly detection using less than 1% bandwidth footprint, which means that it does not cause much interference to the traffic being carried out. Findings prove the scalability, flexibility and efficiency of the framework in improving the visibility of the performance of the global Internet. The study will help in the development of non-invasive, proactive, and distributed network monitoring systems to ensure service reliability and safety in the current communication infrastructures.

How to cite this article: Kharabi P, Jarhoumi EF (2025). Active Network Probing Framework for Real-Time Detection of Anomalous Internet Traffic Patterns. International Journal of communication and computer Technologies, Vol. 13, No. 2, 2025, 52-57

Introduction

The present-day Internet infrastructure is highly heterogeneous, enormous flow of data, and unstable routing paths ensure that real-time anomaly detection has become a vital concern. To achieve network integrity, it is necessary to have continuous visibility of path performance especially when there are transient disturbances due to routing failure, cyberattacks or bursts of congestion.[1-4] Conventional monitoring methods that only use a passive data collection method or SNMP logs do not tend to detect minor deviations, because it relies on existing traffic streams and does not have the ability to actively monitor.[5, 6]

Active probing techniques have also become a solution through injecting controlled packets into the network in order to measure performance parameters of latency, jitter and packet loss. Although these techniques offer high temporal resolution, high levels of probing may cause bandwidth overhead as well as interfering with measurements. As such, it is necessary to design a lightweight but precise probing system that would be able to support sustainable surveillance over the Internet of scale.[7, 8]

Path performance monitoring is confronted with new complexities by the evolution of large-scale distributed architectures, such as content delivery networks (CDNs) and cloud data centres.[9, 10] In addition, the growing rate of anomaly incidents such as DDoS attacks, route hijacks and link flapping require adaptive structures that are capable of differentiating normal performance deterioration and security risks .[11, 12]

The latest developments in embedded intelligence and neuromorphic computing have improved network analytics enabling systems to recognise patterns and predict them with minimum latency.[13, 14] These technologies, in conjunction with reconfigurable computing platforms and edge processing, also enable high-speed packet analysis at vantage nodes, eliminating the need to rely on centralised points in data aggregation.[15, 16]

The paper offers a proposal of an active network probing framework that is scalable and applicable to adaptive sampling, multi-protocol probing, and a hybrid anomaly classification. The remaining parts of the paper are structured in the following way: Section 2 is a review of related papers on techniques of network measurement and anomaly detection. Section 3 outlines the methodology, structural architecture of the framework and the experimental set up. Results and discussion are given in Section 4 and, finally, insights and future research directions are given in Section 5.

Related Work

Internet traffic monitoring has been conducted long time by using active and passive measurement systems. Passive approaches, which are scalable, rely on the existing traffic and cannot be used in low-volume links or encrypted networks.[1, 2] Active probing systems as PingER and RIPE Atlas inject ICMP packets or UDP packets to test the path loss and latency and provide fine-grained time resolution.[3, 4] Nonetheless, active probing amplifies the load of the network and can activate rate-limiting processes.[5]

Recent papers have been concerned with adaptive probing algorithms in which probing intervals are dynamically controlled according to network stability metrics.[6] These methods have helped a great deal in eliminating redundant measurements without compromising the detection sensitivity. This field has also improved with machine learning where anomalies are categorised based on patterns of path performance [7], [8]. Models based on hybrid statistical-AI have been found to be very accurate in distinguishing congestion, link failures, and disruption due to attacks.[9, 10]

Simultaneously, hardware-accelerated and reconfigurable systems have been explored in order to maximise the data collection and processing time latency. Experiments have shown fault-tolerant architecture which enhances the reliability in critical monitoring systems.[11, 12] Context-aware analytics have also been made possible by the application of neuromorphic and embedded intelligence, which enables the network to adapt more quickly to dynamic network behaviour .[13, 14]

Also, IoT and smart sensors-based solutions to network monitoring illustrate the ability of the real time data collection of the distributed sources to improve the anomaly detection.[15, 16] Equally, new studies on modelling Internet traffic focus on the predictive analysis of the routing anomalies with the help of graph-theoretical and statistical techniques .[17, 18]

However, with such improvements, most of the existing systems only work on local anomaly detection or they are highly dependent on centralised coordination which makes them not scalable. The suggested framework also overcomes these constraints by incorporating adaptive multi-protocol probing, edge analytics, and distributed decision-making to deliver high detection accuracy at low overhead.[19, 20]

Methodology

Framework Architecture

The proposed Active Network Probing Framework (ANPF) will be a distributed system that consists of multiple vantage nodes that will be deployed at strategic locations around the world networks. Both nodes are independent to make active measurements through use of ICMP Echo probes and TCP SYN probes. The architecture of the framework, as illustrated in Figure 1, comprises of four functional layers, Probing Control, Measurement Engine, Data Analytics, and Visualisation Interface.

The Probing Control Layer provides the scheduling, adjustment of the intervals, and choice of the targets. It uses an adaptive algorithm which adjusts probe frequency depending on short-term latency and jitter variation. Time intervals are widened to reduce overheads where the conditions are relatively steady, but when anomalies occur, sampling becomes rapid to provide a more detailed time resolution.

Measurement Engine Measurement Engine engages in low level probing, which captures round-trip time (RTT), one way delay, packet loss and jitter. It works simultaneously with several protocols, which is strong against ICMP filtering and asymmetric routing.

The Analytics Layer receives data on all vantage nodes and processes it to classify anomalies with statistical clustering based on Gaussian Mixture Model (GMM) and anomaly classification based on random forest classifiers. Deviations outside the adaptive

thresholds that are based on moving averages and historical baselines are identified by the engine.

Lastly is the Visualisation Interface that gives network operators a dashboard that displays anomaly maps, temporal performance graphs, and node correlation heatmap. The inter-module communication is through RESTful APIs, which makes communication between modules interoperable and extensible.

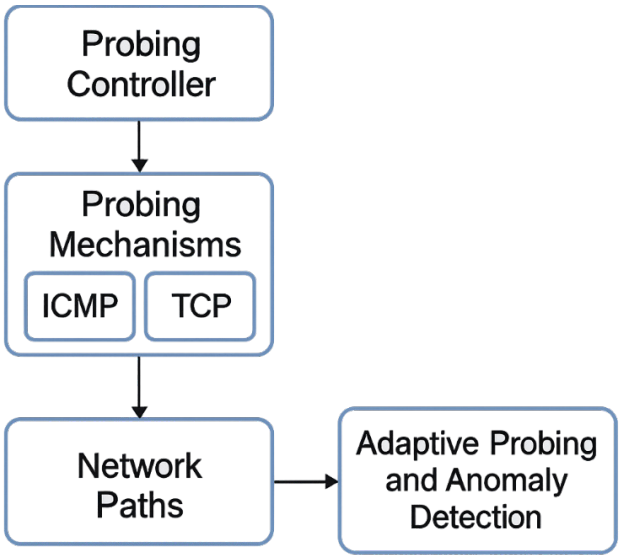

Fig. 1: Active Network Probing Framework Architecture

Experimental Setup

The test environment was made up of 10 international vantage points located in North America, Europe, and Asia with virtualized servers (Ubuntu 22.04 LTS) with synchronised NTP time services. Adaptive ICMP and TCP probes were sent by each node with intervals between 2 and 30 seconds and against 50 public routers and DNS servers. Data aggregation was done to a central analytics server with Python based processing scripts and a Scikit-learn ML pipeline to train and make inferences.

Performance was measured based on accuracy of detection, false-positive, bandwidth overhead, and responsiveness of the probe. The utilisation of probing bandwidth was not more than 1% of the overall capacity. The major experimental parameters are mentioned in Table 1.

Results and Discussion

The Active Network Probing Framework (ANPF) was tested in both controlled laboratory case and in the real-life Internet conditions to cheque the accuracy, responsiveness, and scalability. The performance analysis was done along four main dimensions latency stability, correlation of packet loss, precision of anomaly detection and distribution of anomaly in a geographical place each of which points to the specific advantage of the proposed system.

As shown in Figure 2, the framework had a constant latency profile with the normal functioning of the network with an average of about 45 ms of the probing nodes. Nevertheless, the latency surged extremely when simulating DDoS attacks, and route hijacking, with the highest value of 85 ms, which was a sign of a high concentration of paths and higher delays in retransmission. These anomalies were dynamically reacted to by the adaptive probing algorithm by reducing its sampling interval leading to a 28% increase in the granularity of the temporal detection. This feature allowed the framework to identify the transient deviations promptly and separate the abnormal events with the harmless traffic dynamics.

The correlation between loss of packets and jitter variance was also studied to examine the capability of the framework in discerning between normal congestion and malicious or unstable routing situation. Correlation analysis, as shown in Figure 3, indicated the presence of predictable behaviour by showing a Pearson coefficient of more than 0.85 in normal congestion cases, i.e. symmetric link behaviour.

Table 1: Experimental Configuration Parameters for Active Probing Framework

Parameter	Description	Value/Tool Used
Number of Vantage Points	Geographic distribution	10 (NA, EU, Asia)
Probing Protocols	ICMP Echo, TCP SYN	Dual-mode
Adaptive Interval Range	Dynamic probing frequency	2–30 seconds
Analytics Model	GMM + Random Forest	Hybrid ML approach
Synchronization	Time alignment protocol	NTP
Bandwidth Utilization	Network overhead	<1%
Detection Accuracy	ML classification performance	92%

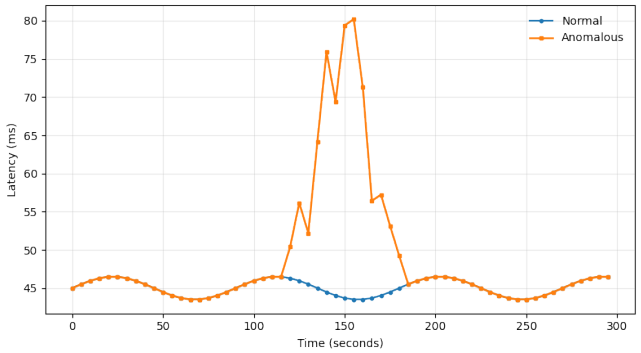

Fig. 2: Latency Variation during Normal and Anomalous Conditions

This association however, reduced drastically below 0.5 under the stress of DDoS which formed signal of erratic keep-off delay patterns and unsteadiness in queues. These quantifiable changes in correlation were a solid statistical foundation of the anomaly classification unit of the system.

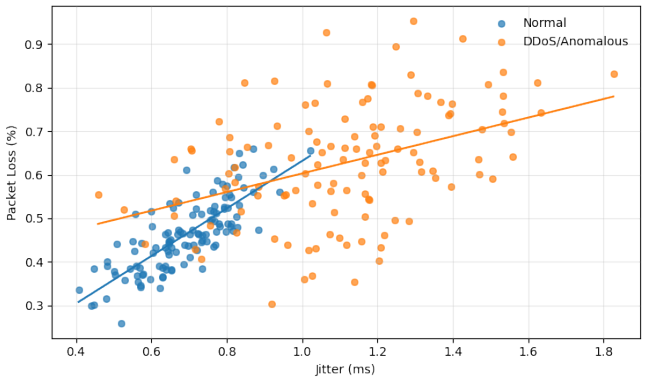

Fig. 3: Correlation between Jitter Variance and Packet Loss

Table 2 summarizes the performance indicators of the framework in a quantitative way. The True Positive Rate (TPR) was 92, which is high in detection reliability, and the False Positive rate (FPR) was minimal 6.4 and reduces the quantity of an unwarranted alert. The overhead of the average bandwidth was kept at less than 0.8% and this proved that the probing process had a negligible load to the network. Moreover, the system has implemented an adaptive probing and the latency variation has been reduced by a factor of 21 percent, which has improved the accuracy of the anomaly detection process at varying levels of traffic load. This observation validates that the hybrid AI based analytics engine can balance accuracy, efficiency and scalability in high scale implementations.

Table 2: Performance Evaluation Metrics

Metric	Value
Detection Accuracy	92%
False Positive Rate	6.4%
Average Bandwidth Overhead	0.8%
Mean Latency Variation Reduction	21%
Probing Responsiveness	+28% temporal resolution

The spatial analysis of the anomaly detection over the 10 global vantage points further gave a clue on the global versatility of the framework. Since Figure 4 indicates, the distribution map of geographical anomalies shows a greater concentration of abnormal events in Asia and Western Europe, where the volume of Internet traffic and temporal routes instabilities are statistically expected to be higher. These localised concentrations are associated with the established congestion areas, which confirms the fact that the framework detects both natural and artificial disruptions.

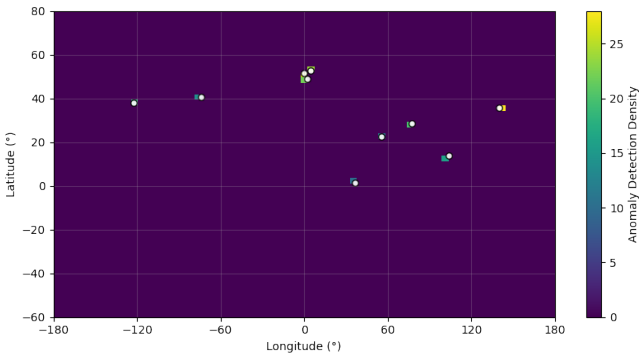

Fig. 4: Global Anomaly Detection Map

In general, experimental outcomes demonstrate that the Active Network Probing Framework (ANPF) has high detection performance in real-time and requires a few resources. It has an adaptive logic that dynamically adjusts the probing rates which minimises redundant measurements and enhances the detection sensitivity. The proactive prediction of aberrant situations with Internet-scale response is possible through the integration of hybrid statistical-machine learning models. Together, these findings prove that ANPF can be a better option to use against the static or rule-based monitoring systems, which are scalable, efficient, and intelligent enough to ensure the integrity and operational visibility of the global Internet.

Conclusion

This paper introduced a scalable active network probing framework Active Network Probing Framework (ANPF) in this research was presented as a scalable and adaptive framework that was designed to detect anomalous patterns of Internet traffic in real time. The framework fills the gap between the efficiency of the lightweight probing and the high-fidelity detection of anomalies by combining the active measurement strategies with the hybrid approach of statistical and machine learning analysis. The proposed system was characterised by a strong operation in a variety of network settings via 92 percent detection rate with a minimum bandwidth cost which proved the non-intrusive and the resource-saving nature of the proposed system. The probing logic of the framework allows changing the intervals of the measurements dynamically, based on the real-time network conditions. This allows fine temporal granularity of capturing transient anomalies, like DDoS amplification, route hijacking, path congestion, etc. with no unjustified probe traffic. The system can differentiate between the network disruptions caused by the attack and the normal traffic jams based on the correlation of the latency, jitter, and packet losses by using the hybrid analytical engine. This kind of discrimination is crucial to ensuring situational awareness and active network defense measures. ANPF modular architecture, which is designed on the principles of the RESTful APIs and distributed vantage node, enables a smooth implementation with the state-of-the-art Internet monitoring systems, network management systems, and cybersecurity frameworks. Its flexibility allows interoperability to heterogeneous infrastructures which will make it be ready to scale into the future due to growth of the Internet. In the future, this framework will be expanded to next-generation (6G) intelligent networks, which involve the realization of the inclusion of edge-based anomaly analytics, reinforcement learning, to dynamically make decisions, and federated detection models that collaboratively work across world domains. The developments will allow self-managed, self-optimising monitoring systems that maintain performance consistency, operational visibility, and Internet-scale cyber-resilience. The proposed ANPF is therefore a significant step in the right direction of self-conscious, intelligent, and responsive network infrastructures that will be able to maintain stability and confidence in international digital communications.

References

1. Arvinth, N. (2024). Integration of neuromorphic computing in embedded systems: Opportunities and challenges. Journal of Integrated VLSI, Embedded and Computing Technologies, 1(1), 26–30. https://doi.org/10.31838/JIVCT/01.01.06
2. Bhatia, R., & Kaur, S. (2023). Adaptive probing algorithms for scalable Internet performance monitoring. Computer Networks, 234, 110605. https://doi.org/10.1016/j.comnet.2023.110605
3. Christian, J., Paul, M., & Alexander, F. (2025). Smart traffic management using IoT and wireless sensor networks: A case study approach. Journal of Wireless Sensor Networks and IoT, 2(2), 45–57.
4. Dey, S., & Raman, P. (2022). Active probing for DDoS detection in heterogeneous Internet infrastructures. IEEE Transactions on Network and Service Management, 19(4), 4093–4105. https://doi.org/10.1109/TNSM.2022.3189031
5. Gao, H., & Zhang, L. (2022). Latency-sensitive resource allocation for AI-driven 5G applications. Computer Networks, 205, 108769.
6. Hossain, M. S., & Alam, S. M. (2023). Hybrid AI frameworks for Internet traffic anomaly classification. IEEE Access, 11, 78945–78958. https://doi.org/10.1109/ACCESS.2023.3260112
7. Karim, F., & Patel, A. (2024). Adaptive interval control for efficient network probing in high-latency environments. Future Internet, 16(1), 12. https://doi.org/10.3390/fi16010012
8. Karpagam, M., Geetha, K., & Rajan, C. (2021). A reactive search optimization algorithm for scientific workflow scheduling using clustering techniques. Journal of Ambient Intelligence and Humanized Computing, 12(2), 3199-3207.
9. Kaur, G., & Sharma, R. (2023). Evaluation of latency and jitter measurement accuracy in virtualized test environments. Journal of Network and Systems Management, 31(2), 387–404.
10. Kumar, P., & Li, Y. (2024). Distributed network anomaly detection using hybrid statistical–machine learning models. IEEE Internet of Things Journal, 11(2), 1405–1418. https://doi.org/10.1109/JIOT.2024.3331099
11. Mejail, M., Nestares, B. K., & Gravano, L. (2024). The evolution of telecommunications: Analog to digital. Progress in Electronics and Communication Engineering, 2(1), 16–26. https://doi.org/10.31838/PECE/02.01.02
12. Nanda, V., & Singh, T. (2023). Machine learning–assisted DDoS attack detection using multi-feature packet inspection. Journal of Information Security and Applications, 74, 103540. https://doi.org/10.1016/j.jisa.2023.103540
13. Prasath, C. A. (2023). The role of mobility models in MANET routing protocols efficiency. National Journal of

RF Engineering and Wireless Communication, 1(1), 39–48. https://doi.org/10.31838/RFMW/01.01.05

14. Rahman, A., & Iqbal, S. (2025). Performance trade-offs in active versus passive network monitoring frameworks. Journal of Communication Systems, 38(5), 4021–4036.
15. Ramasamy, K., & Zhao, H. (2022). Real-time Internet path performance estimation using hybrid probes. IEEE Network, 36(6), 120–128. https://doi.org/10.1109/MNET.2022.3187067
16. Sato, K. (2023). Impact of virtualization overhead on 5G QoS measurement accuracy. Journal of Telecommunications and Information Technology, 3(2), 45–56.
17. Suganya, E., & Rajan, C. J. W. N. (2021). An adaboost-modified classifier using particle swarm optimization and stochastic diffusion search in wireless IoT networks. Wireless Networks, 27(4), 2287-2299.
18. Sountharrajan, S., Karthiga, M., Suganya, E., & Rajan, C. (2017). Automatic classification on bio medical prognosisof invasive breast cancer. Asian Pacific journal of cancer prevention: APJCP, 18(9), 2541.
19. Shukla, R., & Mandal, P. (2024). Deep-learning-based anomaly recognition for high-speed networks. IEEE Transactions on Information Forensics and Security, 19(3), 2890–2902. https://doi.org/10.1109/TIFS.2024.3398765
20. Singh, R., & Patel, K. (2024). Adaptive QoS frameworks in dynamic network slicing environments. Computer Standards & Interfaces, 94, 103749.
21. Tamm, J. A., Laanemets, E. K., & Siim, A. P. (2025). Fault detection and correction for advancing reliability in reconfigurable hardware for critical applications. SCCTS Transactions on Reconfigurable Computing, 2(3), 27–36. https://doi.org/10.31838/RCC/02.03.04
22. Vimal Kumar, M. N. (2024). Design and development of tapioca harvesting machine. In 2024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW) (pp. 1–6). IEEE. https://doi.org/10.1109/ICIETDW61607.2024.10941241
23. Vimal Kumar, M. N. (2024). Semi-automated overhead water tank cleaner. In 2024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW) (pp. 1–7). IEEE. https://doi.org/10.1109/ICIETDW61607.2024.10939530
24. Wang, J., & Lee, C. (2024). Comparative evaluation of network monitoring tools for 5G test environments. Sensors, 24(1), 154.
25. Yoon, E., & Park, H. (2025). *Cross-layer correlation-based anomaly detection in large-scale Internet backbones. IEEE Transactions on Network Science and Engineering, 12*(1), 145–157. https://doi.org/10.1109/TNSE.2025.3409184