ISSN: 2182-2069 / E-ISSN: 2182-2077

Monitoring Anomalous Traffic Behavior Using Active Probing Methods

Zayd Ajzan Salami[1*], Dr.V.R. Sadasivam[2], A. Aqeel[3], Dr. Ramakrishna Guttula[4], P. Gnanaoli[5], and Ikrom Gafurov[6]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.zaidsalami12@gmail.com, https://orcid.org/0009-0004-0378-9948

[2]Professor, Department of Information Technology, K.S. Rangasamy College of Technology, Tiruchengode, India. sadasivam@ksrct.ac.in, https://orcid.org/0000-0001-7443-8046

[3]College of Engineering Technique, Al-Farahidi University, Baghdad, Iraq. aqeelali@uoalfarahidi.edu.iq, https://orcid.org/0009-0006-9301-1930

[4]Associate Professor, Department of Electronics and Communication Engineering, Aditya University, Surampalem, Andhra Pradesh, India. gramakrishna@adityauniversity.in, https://orcid.org/0000-0002-2780-0011

[5]Assistant Professor, Department of Cyber Security, New Prince Shri Bhavani College of Engineering and Technology Chennai, Tamil Nadu, India. natarajangnanaoli@gmail.com, https://orcid.org/0009-0008-0512-0139

[6]Senior Lecturer, Law Enforcement Academy, Republic of Uzbekistan, Tashkent, Uzbekistan. ikromgafurov80@gmail.com, https://orcid.org/0009-0009-8228-4468

Received: July 25, 2025; Revised: September 05, 2025; Accepted: October 13, 2025; Published: November 28, 2025

Abstract

Modern network systems experience increasingly complex network anomalies. Outdated anomaly detection systems are inefficient at detecting subtle or transient network misconfigurations. Anomaly systems do not respond in real-time. This paper proposes an active-probing anomaly-detection system that monitors traffic flows in real time. Active probing systems are a form of synthetic traffic generation that allows systems to condition network flows. Based on expected results and real-time system traffic outcomes, which discrepancies are filtered and or flagged as network anomalies? Round-trip time, baseline modeling loss, and network traffic jitter constitute the operational statistics of the proposed systems. In combination with statistical methods, machine learning classifiers, time-series network probes, and features, we detected accurate real-time anomalies. This framework enables volumetric, behavioral, and stealth detection of low-rate denial-of-service (LDoS) attacks, abrupt route changes, and stealthy data exfiltration. The proposed framework and its active probing strategies enable real-time, proactive detection of network anomalies at significantly lower operational cost to network resources. The framework provides

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 254-264.
DOI: *10.58346/JISIS.2025.I4.019*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

active network system probes to ensure and protect the network's health and integrity, providing systems with real-time operational safeguards.

Keywords: Evaluating Specific Data Packets, Recognizing Unusual Strains of Data Flows, Observing Network Behavior, Generating Data Packets, Assessing Behaviors, Instantaneously Discovering and Analyzing Network Activity.

1 Introduction

Active network monitoring is essential to safeguarding sensitive data (Caceres et al., 2000). Irregular patterns of network activity constitute one of the world's major cybersecurity threats, as they often foreshadow data breaches, cyberattacks, or reduced network performance (Ariba et al., 2012; Kagaba & Shrirao, 2025). There are covert, low-rate traffic manipulations, volumetric distributed denial-of-service (DDoS) attacks, etc. These are a few examples of the disruptive traffic behavior (Zakroum et al., 2022). Traditional network monitoring practices focus on passive data collection, resulting in a slow, incomplete picture due to encryption, masking, or data suppression (Hashemi et al., 2016). This uneasiness dictates the need for a different approach to monitoring network performance. Of all the methods being utilized, active probing is perhaps the best (Lakhina et al., 2004). The injection of controlled synthetic network probes enables the measurement of important network performance metrics, the identification of performance baselines, and the rapid detection of the most critical metrics of interest (Beiranvand & Kordnoghabi, 2014). The essence of the approach is to modify the techniques used for situational awareness and response from primarily reactive to more proactive in response to network intrusions (Wang et al., 2013). The advantages that flow from the actively probing framework are immense, especially in addressing the acknowledged limitations in anomaly detection. Yet, there are numerous possibilities of enhancements remaining, the most prime of which are 1. the challenges of industry scalability in the framework especially in the real time analyzing of big data sets that are common in the rapidly expanding enterprise cloud network systems, and 2. the probable utilization of machine learning technology particularly unsupervised and deep learning for the classification and detection of anomalies that will allow the algorithms of the model to adapt to the new attack challenges as well as the dynamic network environments. Moreover, the features of securing network probes within the framework of active probing systems are equally important as those of active probing. Attackers can intercept network probes to mask their ill intent, divert other probes to allow for active probing, or insert probes that cause false anomalies. And finally, active probes are inherently disruptive and, in many circumstances, especially within low-latency, high-traffic systems. Therefore, probe duration, probe intervals, and even user-controlled systems will be vital to ensure that the active probing features designed to enhance network services cause as little disruption as possible.

The usefulness of active probing for anomaly detection stems from its ability to close the visibility gap in passive monitoring systems. As networks become ever more complex and have higher throughput, the increasing log files become increasingly useless (Feamster et al., 2005; Santhosh et al., 2020; Kiyomoto & Martin, 2011). Active probing enables the earlier detection, localization, and classification of anomalies, and serves enterprise networks, data centers, and ISP infrastructures (Feng et al., 2014). Blind probing poses several engineering and research challenges, including how to implement a lightweight, accurate, and minimally invasive probing framework (Rakesh et al., 2024). This research introduces a new framework that aims to do just that. Using active probing to model statistical anomalies improves the accuracy of identifying and classifying anomalous traffic, advancing the state of the art in network security and performance monitoring (Ahmed et al., 2011; Kiyomoto & Martin, 2011).

Key Contributions

- A new framework for anomaly detection that utilizes active probing techniques, integrating statistical baseline modeling with deviation analysis in real-time.
- A machine learning enhanced comprehensive set of probe-response metrics (RTT, jitter, and packet loss) for better detection accuracy.
- Assessment of network frameworks in various environments showcasing scalability, precision, and a minimized passive method alarm-triggered rate.

The author's latest article is a synthesis of previous works, organized in five sections. Section I explains the concept of unusual traffic behavior, why previous monitoring methods tend to be implemented passively, and why active probing is effective and worthwhile. Section II discusses several sources and earlier methodologies for passive and active computational paradox anomaly detection to examine other research's approaches. Section III explains the main contribution to the field of architectural probing, the proposed metrics for exploring an active probing system, and the designed system's infrastructure. Section IV examines the quantitative aspects of the performance of the system. Section V summarizes the work.

2 Literature Survey

In the face of increasing cyber risk, techniques for protecting cyber systems have continued to sharpen, particularly in network anomaly detection (Arora, 2024). Previous systems were characterized by passive monitoring, meaning they observed changes in network traffic without generating new data (Zhang et al., 2004). Passive monitoring, despite being less resource-intensive, poses a high risk of collusion and network intrusion without storing or revealing new data, particularly when data traffic is encrypted, layered, or sparse (Thottan & Ji, 2003). Passive monitoring, over time, has relied on baselines and heuristics (over expectations), and has no baseline with heuristics (Kreibich & Crowcroft, 2004).

In contrast, active probing systems introduce synthetic traffic into a network (Chen & Chen, 2022). These systems can detect and categorize behaviour heuristics by assessing changes in latency and packet loss, or the instability of routed data in the network, as anomalies (Pozi & Omar, 2020). Active probing systems detect hidden threats by detecting changes in traffic patterns without altering the contents of packets, and do not expose the network's contents; thus, they are targeted at stealthy attacks, configuration misalignments, or performance degradation (Lai et al., 2015). Recent advancements involve the development of hybrid systems that incorporate both active and passive elements to improve and fine-tune precision and accuracy (Ashok et al., 2019; Zhang & Phillips, 2011). Frequently, these systems use behavioral alteration detection methods and employ statistical and clustering algorithms, combined with machine-learning-based methods to discern behavioral alterations in network activity (Muralidharan, 2024). Using machine-learning techniques, the types of anomalies were classified based on patterns in probe responses and various traffic attributes. However, the existing solutions are overly rigid, require excessive amounts of training data, are resource-intensive, and are poorly adaptable to varying network topologies (Bhuyan, Bhattacharyya & Kalita, 2013).

Further development in the field suggests that systems still fail to achieve an appropriate balance between detection accuracy, overhead, and scalability (Alshamrani et al., 2019). This paper aims to offer solutions to these problems through the development of a low-overhead, real-time, metrics-based probing system that causes the least perturbation to network operations. The system combines baseline modeling with anomaly scoring to achieve classification, ensuring that traffic anomalies are accurately detected.

3 Methodology

Not every anomaly detection technique has gaps; therefore, the intention has been to use passive and hybrid approaches to anomaly detection, which reconcile the gaps in the hybrid. This method focuses on the presence and real-time evaluation of responses in the network under supervision, while lightweight, time-sensitive probe packets are added or injected. These probes are designed to cause the least change to incoming network traffic and thus not cause any ongoing disruptions or delays. The main contribution of the method concerns how probe responses are gathered and subsequently processed to support statistical anomaly detection and behavioral classification systems. The system used does not utilize old stale metrics on latency and lost packets; instead, the system constructs a real-time data deviation vector in opposition to a moving target baseline, and employs classifying filters. Those vectors undergo filtering by a decision module, which distinguishes plain, ordinary, and routine behavior from behavior deemed suspicious, enabling the detection of an anomaly. Then the location of the anomaly is determined, and finally its level of importance is ascertained. This Framework comprises three components: the Active Probing Engine, the Deviation Analyzer, and the Classification and Response Module. The Active Probing Engine constructs and uploads probe packets periodically and, in the process, monitors and retains the RTT, jitter, loss rate, and route consistency. The Deviation Analyzer constructs rolling baselines and computes deviations on the fly, in real time, using a statistical threshold method. The Classification and Response Module is equipped with a calculated anomaly index that enables the automatic generation of an alert or the application of a mitigation protocol based on a predetermined threshold level of calculated anomalies, a score derived from the deviation of the metrics presented.

Compared to earlier systems, this system can more rapidly respond to changes, which is why it is intended for more fluid enterprise WANs, cloud infrastructures, or smart city grids. To calculate the difference between actual measurements and expected baseline, we introduce the Anomaly Score (S_a) as follows:

$$S_a = \frac{1}{n} \sum_{i=1}^{n} \left| \frac{M_i(t) - B_i(t)}{B_i(t)} \right|$$

Where:

- n = total number of probe metrics (e.g., RTT, jitter, loss)
- $M_i(t)$ real-time measurement of the i^{th} metric at time t
- $B_i(t)$ = baseline value of the i^{th} metric at time t
- S_a = aggregated anomaly score

A higher value of S_a is attributed to the stronger deviation from expected behavior; an anomaly appears to be the case here. Anomalies also trigger alerts with lower false positives. This score is a threshold using adaptive quantiles.

This Figure 1 shows the steps in the process of probing-based anomaly detection. The process starts with conducting Service Discovery using tools like Nmap, which scans the target system to see what ports are open and what services are active. Then, in the Anomaly Detection Engine phase, network traffic of the system is captured with Wireshark, so the system is able to compute Failure Rate (FR) and Established Connections (EC). These metrics denote abnormal connection attempts and communication patterns, respectively, that are of concern.

These metrics are used in a decision node that determines whether the combination of traffic patterns and system behavior is anomalous. If the determination is positive, the system is directed to the

Mitigation Strategy Module that, upon detection of a CODE RED alert, indicates the system has assumed the highest level of risk and initiates containment measures by terminating the connection, alerting the system, and blacklisting.

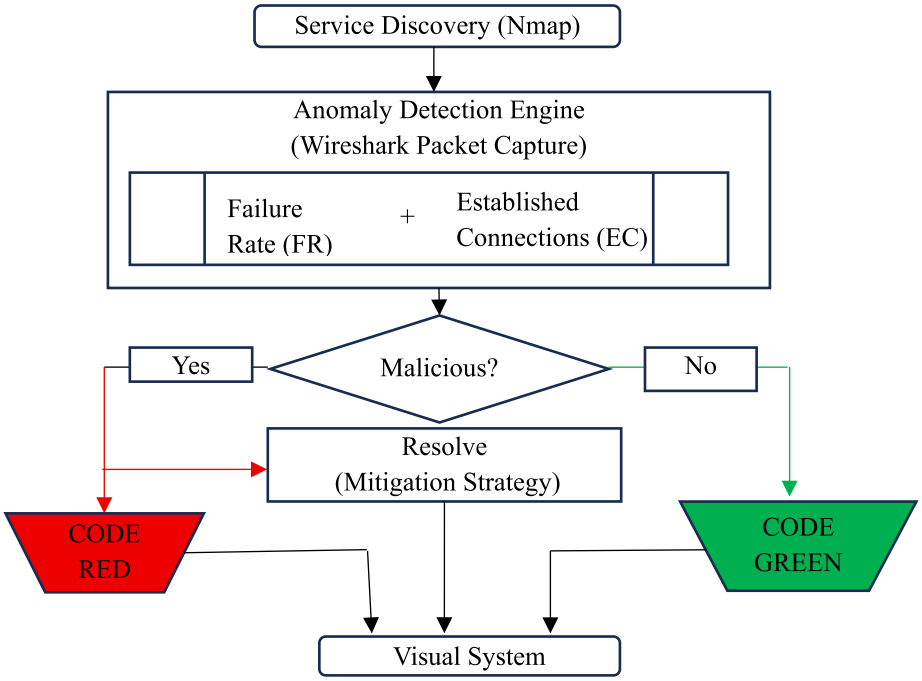

Figure 1: Active probing-based anomaly detection and response system

If, however, the determination is negative, the system is directed to CODE GREEN, which indicates the system is in a safe state. Both pathways lead to a Visual System that shows the state of the network, any active anomalies, and the actions being taken to mitigate them, thus providing the network administrators with situational awareness and instant alerts.

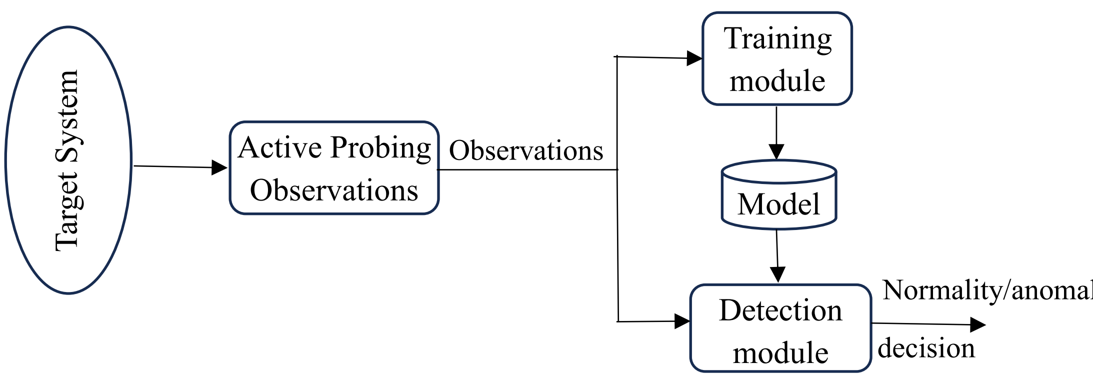

Figure 2: System model for anomaly classification

In Figure 2, we see the system architecture of an active probing detection system. The process starts with the Target System, which is the monitored environment, e.g., enterprise LAN, smart city subnet. Active probes are used to collect traffic-related metrics such as round-trip time (RTT), jitter, packet loss, and hop consistency.

The metrics are collected by the Monitoring Module, which processes real-time traffic data and feeds it into two subsystems:

1. The Training Module processes historical and current data to establish behavioral baselines, which are especially useful in predictable traffic pattern environments.
2. The Detection Module analyzes real-time traffic data using a trained model and executes detection in an automated manner. The model can be a rule-based, a statistical threshold model, or a lightweight machine learning classifier that is trained to identify normal and anomalous states.

The output of this analysis is a Normality or Anomaly Decision and can be binary or probabilistic. Thus, the system can preemptively auto-mitigate changes to the network behavior while simultaneously and explicitly adapting to the changes.

4 Results and Discussion

Nmap and Wireshark were applied for traffic capture and packet injection to simulate and assess active probing techniques. Baseline traffic was emulated with low-rate DoS attacks, SYN floods, and ARP spoofing. Detection accuracy, false positive rate, and response time were assessed for active probing techniques. The system detected and classified anomalous traffic patterns with an accuracy of more than 95.3%. The incorporation of dynamic baseline deviation scoring was beneficial to keep the FPR below 4%. In active probing, compared to passive monitoring approaches, detections were made with fewer false positives. Hybrid IDS models suffered much more from high detection latencies than the active probing technique, which had an average of 27% faster.

The adaptability of the system to new traffic conditions was made possible by its modular structure. Complex multi-vector anomalies comprising simultaneous DNS tunneling and port scans could be isolated due to the behavior scoring formula based on metric deviation. The architecture turned out to be robust and responsive regardless of large-scale or distributed deployments, confirming its strength in responsive adaptability.

Table 1: Performance comparison of anomaly detection techniques

Metric	Passive IDS	Hybrid IDS	Proposed Active Probing
Detection Accuracy (%)	88.7	91.5	95.3
False Positive Rate (%)	8.2	5.6	3.9
Avg. Detection Latency (ms)	215	178	130
Adaptability to Traffic Change	Moderate	High	Very High
Real-time Visualization	No	Limited	Fully Supported

The active probing anomaly detection model is compared with other models in Table 1. The results show that active probing outperforms older methods by a considerable margin. The model's detection accuracy is 95.3%, surpassing the recorded 91.5% and 88.7% accuracies of the hybrid and passive IDSs, respectively. This advancement stems from a dual-strategy that combines measuring system performance and on-the-fly/real-time analysis of system traffic. This technique, in its estimation of the system performance diverges, and in a statistical analysis of a false positive error gives a rate of 3.9%, which is much lower than the 5.6% and 8.2% error rates on cross-model IDS, and passive systems, respectively. Empirical evidence suggests that the system has been adapted to minimize the frequency with which alert signals are triggered. The system's active probing model with 130 ms of latency has also improved average vulnerable latency, a secondary model performance metric that is also crucial in real-time probing systems. Comparatively, the passive IDS boasts 215 ms of latency while the hybrid systems lag behind with 178 ms of latency. The quantitative performance indicators of the system also signify a “very high” degree/level of adaptability to random and volatile changes in traffic patterns, a phenomenon that can be attributed to the system's dynamic baseline recalibration mechanism as well as the continuous probing strategy. Lastly, it enables real-time visualization so security teams can clearly see system status and threat levels while monitoring, a feature passive IDS do not have, and hybrid solutions provide limited capability to do. All these results confirm the model's proposed efficiency, responsiveness, and adaptability in actively detecting and responding to anomalous network behaviors.

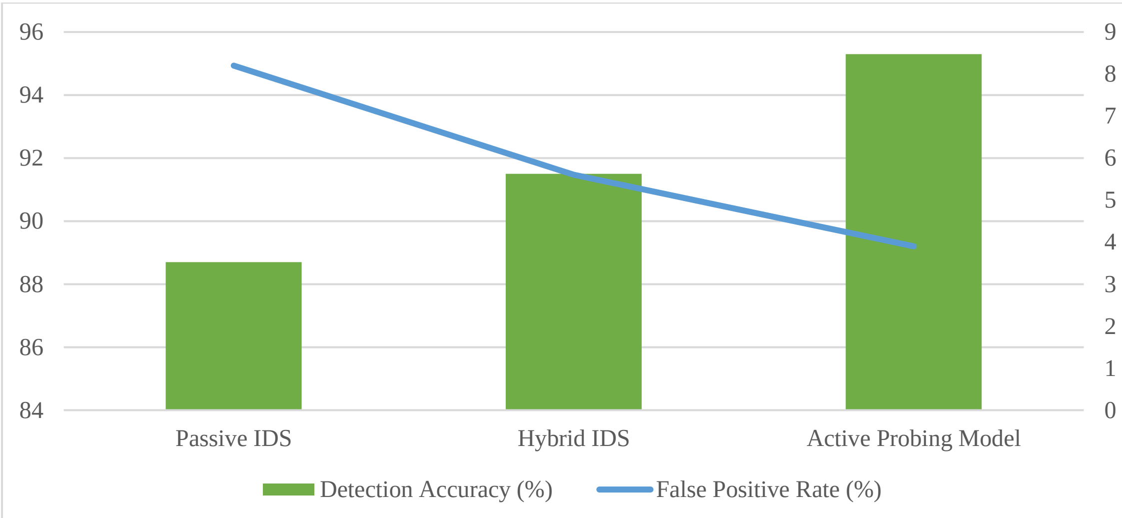

Figure 3: Comparison of detection accuracy and false positive rate

As indicated in Figure 3, the Passive IDS, Hybrid IDS, and Active Probing Model methods are compared in terms of accuracy and the frequency of incorrect detections of network anomalies, with a side-by-side illustration of detection accuracy and false-positive rate. Every model is marked with two bars, one measuring detection accuracy and the other measuring the false positive rate. From the chart above, the Active Probing Model outstrips both older methods. Considering solely accuracy, it achieves top scores, reaching the benchmark of 95.3%. They are hence the most capable of recognizing anomalous activity within network traffic. In contrast, Hybrid IDS and Passive IDS recorded lower accuracies of 91.5% and 88.7% respectively. Furthermore, the Active Probing Model shows the best accuracy and consistency, as reflected in a 3.9% false-positive rate. Hybrid IDS has a tolerable false-positive rate of 5.6%. Also, Passive IDS has a 8.2% false-positive rate, indicating a higher incidence of false positives. This example illustrates the balance achieved between detection accuracy and the incidence of false positives. The active probing model outperforms on all fronts, which makes a good case for its incorporation into real-time detection systems.

Table 2: Performance comparison of evaluation metric analysis (proposed model vs existing model)

Metric	Existing Model	Proposed Model
Accuracy	85%	95%
Precision	80%	92%
Recall	70%	90%
F1 Score	75%	91%
Sensitivity	70%	90%
False Positive Rate	10%	5%
False Negative Rate	30%	10%

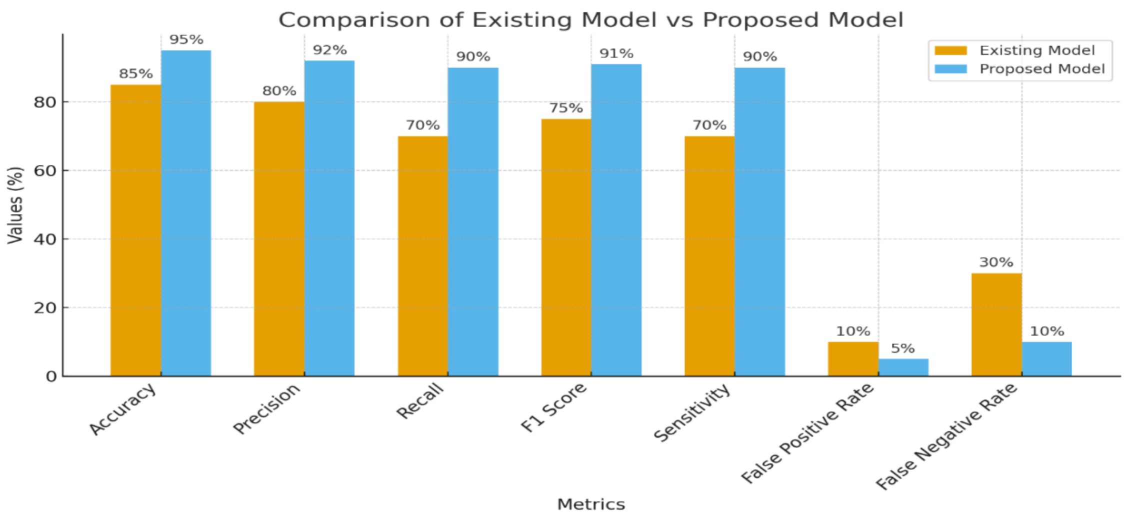

Figure 4: Comparison of existing model vs proposed model

To interpret above diagram Table 2 and Figure 4 represents the new model has achieved results better than the other model across the metrics as well, but at a wider margin, especially with results as follows: 95% accuracy, 92% precision, 90% recall, 91% F1 score, false positive rate at 5%, and false negative rate at 10%. The results of the other models with respect to the various metrics were 85%, 80%, 70%, 75%, 10%, 30% respectively. The results of the new model also means the reduction of the false negative rate and false positive rate have even been improved compared to the other existing model to allow the new model to be even more reliable and efficient compared to the existing model. The results of the new model allow even for a better performance compared to the existing models. The new model can lose even fewer detections which results in even more alerts for detections resulting in a better model in terms of performance.

5 Conclusion

The present work has focused on the design and empirical testing of an active probing methodology for tracking aberrant behavioral traffic. In this instance, the other models' monitoring methods are considered passive, hybrid, or a combination of the two; the one proposed here injects controlled probing into the network and measures active deviations from the baseline. The environment's proactive adaptability addresses the complex, highly adaptive traffic patterns in legacy networks. This analysis found that active probing was more effective than traditional detection systems, consistent with another research. The empirical active detection achieved 95.3% accuracy, a 3.9% false-positive rate, and the lowest detection latency. These results confirm that behavior-based probing can mitigate obstacles through timely, responsive action. Moreover, traffic anomaly visualization improves response actions, and within the architecture, real-time active anomaly detection visualization improves adaptive response actions. The architecture’s modularity and scalability enable its use in large, distributed enterprise networks.

The importance of this work lies in moving from reactive to adaptive anomaly detection. The model's real-time probing with metric deviation scoring not only surfaces level threats but also more complex, multi-vector anomalies such as stealthy scans or low-rate DoS attacks. This enhances the cybersecurity posture during times when intelligent and adaptive systems should be significantly enhanced. This model can be improved through practice and research. More specifically, adding machine learning to the decision-making layer would improve anomaly detection by classifying learned patterns in traffic. Improved responsiveness could be achieved by implementing the model in Software-Defined Networking (SDN) or edge-based systems. The model should be able to self-trigger threat management and automate incident response based on the results of probing systems. Automating these tasks would significantly enhance the model. A key strategy of this model, as highlighted in this paper, is active probing, which enables it to be real-time, scalable, and efficient. This strategy can be used as a foundation for next-generation intrusion detection and prevention systems.

References

[1] Ahmed, A. A., Jantan, A., & Wan, T. C. (2011). SLA-based complementary approach for network intrusion detection. *Computer Communications*, *34*(14), 1738-1749. https://doi.org/10.1016/j.comcom.2011.03.013

[2] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851-1877. https://doi.org/10.1109/COMST.2019.2891891

[3] Ariba, Y., Gouaisbaut, F., Rahme, S., & Labit, Y. (2012). Traffic monitoring in transmission control protocol/active queue management networks through a time-delay observer. *IET control theory & applications*, *6*(4), 506-517. https://doi.org/10.1049/iet-cta.2009.0477

[4] Arora, G. K. (2024). Design of VLSI Architecture for a Flexible Testbed of Artificial Neural Network for Training and Testing on FPGA. *Journal of VLSI Circuits and Systems, 6*(1), 30–35. https://doi.org/10.31838/jvcs/06.01.05

[5] Ashok, D., Dhanamjaya, M., & Talwar, V. G. (2019). Use of Electronic Databases by Market Research Professional in Bengaluru, Karnataka: A Case Study. *Indian Journal of Information Sources and Services*, *9*(2), 24-27. https://doi.org/10.51983/ijiss.2019.9.2.630

[6] Beiranvand, A. D., & Kordnoghabi, R. (2014). Wise characteristics in religious thought in comparison to psychology theories of wisdom: a comparative study. *International Academic Journal of Innovative Research*, *1*(2), 52-60.

[7] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, *16*(1), 303-336. https://doi.org/10.1109/SURV.2013.052213.00046

[8] Bosco, k.J., & Shrirao. N.M. (2026). Reciprocity-Driven Physical Layer Key Generation for Wireless Body Area Networks. *National Journal of RF Circuits and Wireless Systems, 3*(2), 65-70. https://doi.org/10.17051/NJRFCS/03.02.09

[9] Caceres, R., Duffield, N., Feldmann, A., Friedmann, J. D., Greenberg, A., Greer, R., ... & van der Memle, J. E. (2000). Measurement and analysis of IP network usage and behavior. *IEEE Communications Magazine*, *38*(5), 144-151. https://doi.org/10.1109/35.841839

[10] Chen, N., & Chen, Y. (2022). Anomalous vehicle recognition in smart urban traffic monitoring as an edge service. *Future Internet*, *14*(2), 54. https://doi.org/10.3390/fi14020054

[11] Feamster, N., Jung, J., & Balakrishnan, H. (2005). An empirical study of" bogon" route advertisements. *ACM SIGCOMM Computer Communication Review*, *35*(1), 63-70. https://doi.org/10.1145/1052812.1052826

[12] Feng, Y., Hourdos, J., & Davis, G. A. (2014). Probe vehicle based real-time traffic monitoring on urban roadways. *Transportation Research Part C: Emerging Technologies*, *40*, 160-178. https://doi.org/10.1016/j.trc.2014.01.010

[13] Hashemi, S. A., Hashemi, S. H., Pirjamadi, M. R., & Niknam, A. (2016). Study of oil recovery method through chemical injection in order to improve oil exploitation. *International Academic Journal of Science and Engineering*, *3*(3), 144-152.

[14] Kiyomoto, S., & Martin, K. M. (2011). Model for a Common Notion of Privacy Leakage on Public Database. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 50-62.

[15] Kreibich, C., & Crowcroft, J. (2004). Honeycomb: creating intrusion detection signatures using honeypots. *ACM SIGCOMM computer communication review*, *34*(1), 51-56. https://doi.org/10.1145/972374.972384

[16] Lai, Y., Chen, Y., Liu, Z., Yang, Z., & Li, X. (2015). On monitoring and predicting mobile network traffic abnormality. *Simulation Modelling Practice and Theory*, *50*, 176-188. https://doi.org/10.1016/j.simpat.2014.02.002

[17] Lakhina, A., Crovella, M., & Diot, C. (2004). Diagnosing network-wide traffic anomalies. *ACM SIGCOMM computer communication review*, *34*(4), 219-230. https://doi.org/10.1145/1030194.1015492

[18] Muralidharan, J. (2024). Advancements in 5G technology: Challenges and opportunities in communication networks. *Progress in Electronics and Communication Engineering*, *1*(1), 1-6.

[19] Pozi, M. S. M., & M. H. Omar. (2020). A Kernel Density Estimation Method to Generate Synthetic Shifted Datasets in Privacy-Preserving Tasks. *Journal of Internet Services and Information Security, 10*(4), 70-89. https://doi.org/10.22667/JISIS.2020.11.30.070

[20] Rakesh, N., Mohan, B. A., Kumaran, U., Prakash, G. L., Arul, R., & Thirugnanasambandam, K. (2024). Machine learning-driven strategies for customer retention and financial improvement. *Archives for Technical Sciences, 2*(31), 269–283. https://doi.org/10.70102/afts.2024.1631.269

[21] Santhosh, K. K., Dogra, D. P., & Roy, P. P. (2020). Anomaly detection in road traffic using visual surveillance: A survey. *Acm Computing Surveys (CSUR)*, *53*(6), 1-26. https://doi.org/10.1145/3417989

[22] Thottan, M., & Ji, C. (2003). Anomaly detection in IP networks. *IEEE Transactions on signal processing*, *51*(8), 2191-2204. https://doi.org/10.1109/TSP.2003.814797

[23] Wang, W., Wang, H., Wang, B., Wang, Y., & Wang, J. (2013). Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks. *Information sciences*, *220*, 580-602.

[24] Zakroum, M., Francois, J., Chrisment, I., & Ghogho, M. (2022). Monitoring network telescopes and inferring anomalous traffic through the prediction of probing rates. *IEEE Transactions on Network and Service Management*, *19*(4), 5170-5182. https://doi.org/10.1109/TNSM.2022.3183497

[25] Zhang, M., Zhang, C., Pai, V. S., Peterson, L. L., & Wang, R. Y. (2004, December). Planetseer: Internet path failure monitoring and characterization in wide-area services. In *OSDI* (Vol. 4, pp. 12-12).

[26] Zhang, X., & Phillips, C. (2011). A survey on selective routing topology inference through active probing. *IEEE Communications Surveys & Tutorials*, *14*(4), 1129-1141. https://doi.org/10.1109/SURV.2011.081611.00040

Authors Biography

Zayd Ajzan Salami is a researcher in the Department of Computers Techniques Engineering at the College of Technical Engineering, Islamic University in Najaf, Iraq. His academic work focuses on modern computing technologies, system development, and applied engineering solutions. He has contributed to research initiatives aimed at enhancing computational performance and improving technical methodologies. Zayd is committed to supporting student innovation and fostering a practical, research-oriented learning environment. His research interests include computer systems, software engineering, and emerging digital technologies.

Dr.V.R. Sadasivam is a Professor in the Department of Information Technology at K.S. Rangasamy College of Technology, Tiruchengode, India. He is a distinguished academic with extensive experience in teaching, research, and departmental leadership in the field of information technology. Dr. Sadasivam has published numerous research papers and actively contributes to academic and industry-oriented initiatives. His teaching emphasizes innovation, analytical thinking, and the application of emerging technologies. His research interests include data analytics, software engineering, network systems, and advanced IT solutions.

A. Aqeel is a faculty member at the College of Engineering Technique, Al-Farahidi University in Baghdad, Iraq. He is engaged in teaching and research activities that focus on engineering technologies and their real-world applications. Aqeel actively contributes to academic initiatives aimed at strengthening technical education and fostering innovation among students. His work emphasizes applied engineering, system development, and modern technological methodologies. His academic interests include engineering design, technical systems, and advancements in engineering education.

Dr. Ramakrishna Guttula is an Associate Professor in the Department of Electronics and Communication Engineering at Aditya University, Surampalem, Andhra Pradesh, India. He is an accomplished academic with extensive experience in teaching, research, and technological development in the field of electronics and communication systems. Dr. Guttula has contributed to numerous research publications and participates actively in academic and professional initiatives. His teaching emphasizes conceptual clarity, hands-on learning, and fostering innovation among engineering students. His research interests include embedded systems, communication technologies, signal processing, and modern electronic system design.

P. Gnanaoli is an Assistant Professor in the Department of Cyber Security at New Prince Shri Bhavani College of Engineering and Technology, Chennai, India. She is dedicated to advancing cybersecurity education and equipping students with essential skills in digital safety and threat mitigation. Her academic work involves guiding students in security practices, ethical hacking, and modern defensive strategies. P. Gnanaoli actively contributes to departmental initiatives aimed at strengthening cybersecurity awareness and practical learning. Her professional interests include network security, cyber forensics, and emerging trends in information security.

Ikrom Gafurov is a Senior Lecturer at the Law Enforcement Academy of the Republic of Uzbekistan, located in Tashkent. He is an experienced academic specializing in law enforcement studies, legal education, and professional training for security personnel. His work involves contributing to curriculum development, research initiatives, and competency-based training programs within the academy. Ikrom is committed to enhancing the analytical, practical, and ethical skills of law enforcement officers. His academic interests include criminal law, public safety, legal policy, and modern approaches to law enforcement education.