World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Research Article)

Autonomous network monitoring using LLMs and multi-agent systems

Oluwatosin Oladayo Aramide *

Network Engineer (Network Layers and Storage) – MTS IV, IRELAND.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 974-985

Publication history: Received on 16 November 2024; revised on 24 December 2024; accepted on 30 December 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.2.0639

Abstract

This study researches the combination of the concept of large language models (LLMs) and multi-agent systems implementation into autonomous network monitoring. Dedicated to real-time anomaly detection in network telemetry (NetFlow, SNMP, GNMI), the study analyzes the possibility of GPT-based agents in efficiently identifying and responding to a network problem. The study also explores some details of Lang Graph and Auto Gen in construction of multi-agent systems to triage and remediate the network events. A case study on automating Root Cause Analysis (RCA) in spine-leaf topologies illustrates the practical application of these technologies. The results indicate that the detection of anomaly is quite efficient in speed, accuracy, and scalability and serve as a rather efficient way of simplifying network operations. The paper highlights, as the recognition of the role of AI in NetOps increases, the potential of converting network management with enhancements to automation and decision-making processes that LLMs and multi-agent systems provide. The implications are huge in terms of the future of NetOps where network infrastructures can be smarter and self-healing.

Keywords: Anomaly Detection; Network Telemetry; Multi-Agent Systems; Event Triage; Root Cause; AI-Driven

1. Introduction

Over the last several decades, network monitoring technologies have changed greatly and moved on to more automated, proactive solutions compared with those known as reactive and manual. At the early stage of the development of network monitoring tools, most of the attention was directed at the traffic flow analysis, simple network failure detection and on measuring uptime. More advanced tools were however needed as networks became more complex and distributed. Artificial Intelligence (AI) and Machine Learning (ML) have since revolutionized the field, enhancing network monitoring by providing real-time data analysis, predictive capabilities, and anomaly detection. The technology embedded in AI-based solutions has become a part and parcel of detector of complicated network behavior and anticipate any problematic occurrences before they can affect the network functions. Network telemetry is an important component of this transformation, and in this respect, anomaly detection in network telemetry, which is provided by such technologies as NetFlow, SNMP, and GNMI can help to obtain and process the information about network performance. Machine learning algorithms are particularly effective in analyzing large datasets to identify abnormal patterns, improving efficiency and network reliability (Waqas et al., 2022). As the networks become more complex, the anomaly detection systems may offer an early warning regarding the possible problems, e.g. the network is congested, attacked, or the equipment fails, hence limiting the number of downtimes and enhancing the system performance (Sivalingam, 2021).

1.1. Overview

The combination of LLM and multi-agent systems is a game changer in autonomous network monitoring because they make smart and self-effective systems that could learn and identify and act based on real-time events in the network.

* Corresponding author: Oluwatosin Oladayo Aramide

Agents in the GPT-based and LLMs category use natural language processing to decipher any data in a network, whereas multi-agent systems offer decentralized decision-making competency, and multiple agents can coordinate to correct and fix issues on a network (Calegari et al., 2020). Such technologies have the capability of triaging network events autonomously, using telemetry protocols like NetFlow, SNMP, and GNMI to collect and analyze data. NetFlow can be used to analyze the traffic flow, SNMP is critical in managing the network, and GNMI makes it easy to configure the network devices, which makes everything necessary to build the complete world of monitoring. Regarding the multi-agent systems, agents either coordinate with or act as individual entities, with the use of logic-based technologies to achieve effectiveness on the network operation. Such systems are also capable of resource allocation and task scheduling, similar to applications in smart grids (Binyamin & Ben, 2022). The end-to-end solution provides a more dynamic, scalable placement on how to control network problems which makes sure that the problems are dealt with in real time with minimum human efforts.

1.2. Problem Statement

Conventional monitoring systems in networks have a number of deficiencies like high delay in detecting and responding to network irregularities, low rate of handling large networks and the need to reflect manual dexterity in resolving troublesome situations. Though existing AI-based surveillance mechanisms show better speed and accuracy, they are yet to perform well under real-time anomaly identification in dynamic networks and high-traffic networks. Most systems are not capable of prioritizing events or performing fixes on their own without any human intervention. Moreover, the current solutions do not give profound insights on various network protocols and telemetry data at large a time, hence missing spaces in discovering and rectifying more complex network outages. This study will hence focus in filling these gaps by considering the use of advanced AI and multi-agent systems in providing an improved monitoring and reaction that is fast and automated, to effectively control complex networked environments.

Objectives

The given study will examine the opportunities of using GPT-based agents in live anomaly detection, studying how well such agents are capable of autonomously detecting and responding to the problems on the network. Evaluation of the construction of multi-agent systems, capable of triaging network events, prioritizing issues and automatically triggering remedial operations using Lang Graph or Auto Gen is another important goal. Additionally, the research will demonstrate the automation of Root Cause Analysis (RCA) in spine-leaf network topologies, a critical task in large-scale network management. Automation of the RCA can help the study to increase the efficiency of network operations, decrease downtime, and increase overall resilience of the network in general; the potential of the AI-driven solutions in network monitoring can be demonstrated by the automation of RCA.

1.3. Scope and Significance

This research focuses on enhancing real-time monitoring, event triaging, and Root Cause Analysis (RCA) automation within complex network environments. This is done by engaging GPT-based agents and multi-agent systems, through which the research targets to develop a more effective and independent solution to manage a network. The findings will contribute significantly to the future of AI in Network Operations (NetOps), positioning AI as a transformative force in network performance and reliability. This research would be useful to scientists as well as practitioners since it provides a new understanding of the practical implications of AI in network operations, especially anomaly revelation, event defection and root go at. It also claims to simplify network administration and prevention of human intervention resulting to resilient and scalable network infrastructures.

2. Literature Review

2.1. Autonomous Network Monitoring

The concept of network monitoring technologies has had a history since the very mere traffic analysis tools are up to a more sophisticated real-time system capable of handling a modern network. Conventional approaches were handled by manual adjustment and regular reviews, which did not, in most cases, deliver the relevant information in handling the networks. At this point, AI- and machine-learning-drives autonomous network performance and monitoring systems are able to continuously monitor network traffic as well as other network performance metrics in real-time. Such systems apply the protocol such as NetFlow, SNMP, or GNMI, as a method of receiving telemetry data and automatically analyzing events regarding the network, resulting in the increased quickness and efficient deviation reviewing. Self-governing systems would be important in minimizing the input of human powers in controlling the network hence more effective control. With AI-powered systems it is possible to automatically identify anomalies, detect possible vulnerabilities and even repair themselves (redistributing traffic or changing settings) without human intervention.

Independent network monitoring is significant by virtue of scaling up in the complexity of contemporary networks and at the same time providing real-time features and quick reactions on the network problems. The growing use of the AI and machine learning is as the internal part of the network security and performance maintenance, which Fuentes-Garc2A‡a et al. (2021) underline by saying that intelligent systems can be used to eventually monitor network security. Not only do these systems enhance the efficiency of operations but also offer proactive security, including identifying the threats in advance (Musumeci et al., 2019).

2.2. Network operations with Large Language Models (LLM)

Large Language Models (LLMs) already have many uses in different sectors, and their use in networks becomes increasingly popular. LLMs like GPT-based agents, can also use much information at once in the form of unstructured data transmitted across the network, which makes the anomaly detection and handling stellar. Those can read and write in a human-like way, so they can be used to help in decoding complex telemetry on networks and to open-up the management of network-related events. Earlier utilization of LLMs in network management has been mostly used to automate the process of identifying security breaches and other anomalies on the network via the analysis of textual data stored in log files and alerts amongst other data on the network. The possibilities of GPT-based agents on the use of network monitoring systems have been evidenced of identifying anomalies at real-time based on pattern detection of data and instrumental in offering actionable information. According to Luise and Denean (2021), LLMs are the cutting-edge technology in the field of AI application development, and one of the examples demonstrating potential efficiency and the minimization of human supervision over the complex network is the task of using them in network activities. With the help of the LLMs, the network events can be classified and prioritized by the network managers in an automated manner, which enables them to manage network resources and network security more effectively and responsively. These developments indicate how the future network monitoring system will look like, fully intelligent yet able to regulate itself to the varying situation on the network without requiring any human assistance.

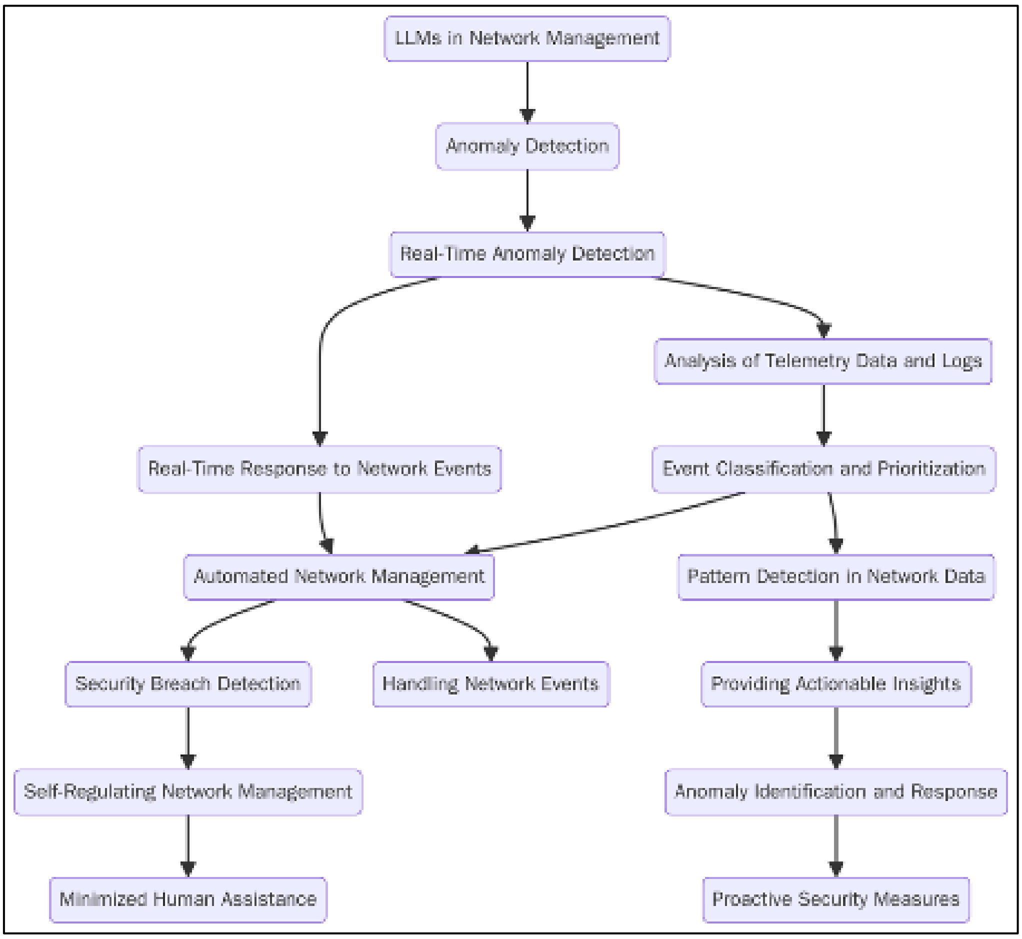

Figure 1 Flowchart illustrating Network Operations with Large Language Models (LLM)

2.3. Multi-Agent Based System in Network Monitoring

Multi agent systems (MAS) are important features of network enhancement through which complex tasks using decentralized collaborative solutions can be met. During network monitoring, MAS facilitates the interaction of multiple agents, information sharing and event detection, triaging, and remedial activities. One of the major benefits of MAS is that the workload can be shared among several agents thus enhancing flexibility and scalability. Agents may work alone or would cooperate in real time to resolve network events, resulting in faster detection and resolutions of network events. Auto Gen and Lang Graph, Multi-agent architecture work really well when it comes to automating network processes. Logic-based agent Lang Graph can be used to create distributed agents that can learn and reason over the network conditions and Auto Gen creates agents to discover solutions to complex network problems autonomously. These structures greatly enhance the effectiveness of the operation of the networks as they tend to automate some of the processes like the routing of traffic, load balancing, and network security monitoring which are conducive to inefficient operations.

Dorri et al. (2018) argue that MAS is capable to provide answers to the network monitoring problems, implementing scalability and flexibility to the problems and responding dynamically to the changes in the network. Moreover, Herrera et al. (2020) pinpoint the beneficial role of MAS in handling complex network management, particularly, in systems engineering where the multi-agent cooperation may ease the work of managing large scale and distributed networks.

2.4. Anomaly Detection in Network Telemetry

Network-telemetry anomaly detection is important to alert against traffic congestion and security breaches and predict network system failure in real-time. Current security tools to identify anomalies in telemetry data, such as NetFlow, SNMP, and GNMI, study traffic patterns in the network and compare it to a set of known standards or learn the behavior of the network and identify unusual changes in it. Although these techniques have achieved remarkable success, they continue to encounter the challenge of timely detection and effective mitigation of the anomalies especially in the dynamic and large-scale networks. Take an example of anomaly detection; in many cases, it is difficult to detect the anomaly where the volume of information on the network is high, thus there are delays in recognition of a future problem. Also, network environments continuously change and this makes the traditional systems incapable of adapting to these changes within a short period. Nam et al. (2020) propose a recurrent neural network (RNN)-based approach to in-band network telemetry for detecting anomalies in real-time, addressing some of these challenges by enhancing the speed and accuracy of anomaly detection. Similarly, Zhang et al. (2022) focus on automating rapid network anomaly detection using in-band telemetry, demonstrating how advanced techniques can improve both the efficiency and scalability of anomaly detection systems. Notwithstanding these developments, the task continues to provide solutions with the ability to rapidly and accurately detect complex anomalies in real time through which they can be swiftly mitigated and network services as curtailed as possible.

2.5. Root Cause Analysis in Networking

Root Cause Analysis (RCA) for network failures is a critical process for identifying and addressing the underlying issues in complex network environments. Conventional RCA approaches are usually based on hand interventions and simple types of diagnostics, e.g. RCA viewing log files, RCA event correlation and RCA rule-based systems. Though, they can be applied in the case of straightforward network breakdowns, these methods may fall short in case of multi-layered issues characteristic of contemporary network design, including spine-leaf designs. The tremendous amount of data that users have on their networks coupled with the dynamism of network conversions make it not easy to ascertain the cause of the problem within a short duration making the site experience high and undesired downtimes with the solution being wasteful. An AI based solution, however, is more proactive instead, in that it is able to automate the detection and diagnosis of the problem. Techniques like machine learning (ML) and deep learning (DL) enable these systems to continuously learn from network data and identify patterns that are indicative of underlying problems, improving both accuracy and speed. Qiu et al. (2022) use the context of adding AI into the Net-RCA of the future 6G networks and focus on the fact that AI can independently discover and fix network failures by matching various types of data. Also, Franklin et al. (2022) discuss the idea of how the machine learning-based closed-control loops will facilitate RCA in Beyond 5G multi-domain networks, which will be more resilient and scalable than managing the network failure in this way. Unlike traditional methods of RCA, AI-based approach is more dynamic and efficient, which leads to considerable saving of the time and resources spent on the identification and resolution of the network problems.

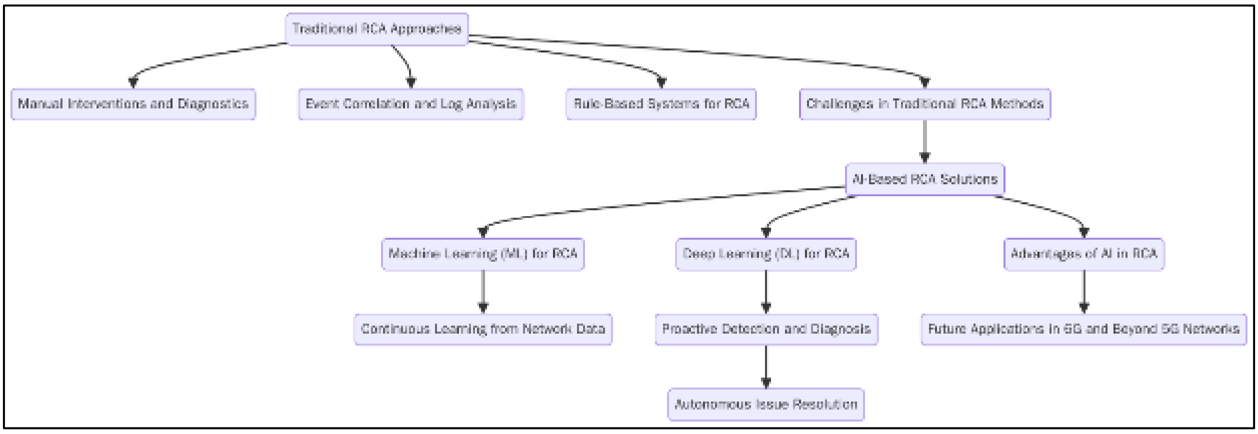

Figure 2 Flowchart illustrating Root Cause Analysis (RCA) in Networking

3. Methodology

3.1. Research Design

The study covers a mixed method with a qualitative and quantitative analysis to give a complete study of autonomous network monitoring with the use of AI and multi-agent systems. The quantitative side is aimed at gathering and processing network telemetry data, like NetFlow, SNMP or GNMI, to seek the patterns, derive anomalies, as well as measure the system performance. In order to evaluate the rate of effective GPT-based agent and multi-agent system performance in real-time anomaly detection and event triage, statistical analysis will be applied. It has qualitative aspect that entails case studies and expert interviews which will enable them to give detailed knowledge concerning the operational difficulties and advantages to integrating the use of these AI-driven mechanisms within actual network settings. The mixed-methods research design provides a balanced outlook on the subject, since the view of the data is complemented by the shift toward qualitative interviews, allowing a deeper grasp of the issue of AI potential and its role in network operations.

3.2. Data Collection

The data that will be used in this study will mainly comprise network telemetry data, e.g., NetFlow, SNMP, gNMI which will offer substantial information on the traffic, status of the devices as well as performance data in the network. NetFlow tracks the patterns of traffic on the network i.e. source and destination IP, protocol and port numbers. SNMP offers device-level status and data, such as CPU loads, memory usage, and interface livingness. gNMI gathers data pertaining to the network device on a per-second basis, which allows viewing the network topology and monitoring the device configurations. The techniques of collecting this data will entail the utilization of network monitoring tools, which are compatible with these protocols, hence the persistent harvesting of telemetry data. Also, information of the abnormalities will be collected based on event logs or alert systems and real-time monitoring dashboards, and the information will be analyzed to identify the presence of unusual patterns or failures.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Automating RCA in Spine-Leaf Topologies

The spine-leaf design is growing rapidly to be popular architecture in modern network infrastructures because of its properties: scalability, extensibility and its low-latency design. But the more complex the networks are, the more complex the problem in finding, identifying and troubleshooting network problems effectively becomes. Root Cause Analysis (RCA) in spine-leaf topologies traditionally involves manual investigation, which can be time-consuming and prone to human error. AI and by extension machine learning algorithms would help automate RCA in such complex systems and this solution would be powerful in addressing such issues.

In a common spine-leaf set up, the spine switches will be charged with the carriage of the traffic between various leaf switches, which will be linked to the said end machines. Any fault in this elaborate arrangement of a complex otherwise may cause the severe degradation of services and it may be highly difficult to identify the fault as also because the devices and traffic flows are closely interdependent. The conventional approach to the RCA usually presupposes manually sorting logs and network telemetry, as well as device status lists, which is time-consuming and exhaustively requires high-level knowledge. Also, as networks become larger and more dynamic, this manual system of network management is even less realistic and unworthy of a contemporary network.

AI-driven systems are used to provide a real-time analysis of telemetry data in the network to automate RCA in spine-leaf topologies. These systems use protocols like NetFlow, SNMP and gNMI to collect performance data of devices on the network and traffic flows. ML models are trained to identify the anomalies and patterns in real time, which allows the system to alert about problems before they could turn into a service shutdown. Once an anomaly has been identified, the AI system has the ability to identify the root cause of the issue by correlating the data on the telemetry of the entire network and considering such factors as device health, traffic jams and network set up.

By automating RCA, network engineers can reduce the mean time to repair (MTTR) significantly, as the system provides immediate insights into the nature of the failure and its exact location within the network. As an example, when there is congestion in a certain leaf switch or a spine switch failure, the AI system will be able to detect these problems, see the patterns in traffic and see device states. This allows the network operations staff to move quickly to correct the problem, with rerouting traffic or reconfiguring the devices, to lessen the performance effects on users.

The leading advantage of the given strategy is that it can be run on an independent basis, almost without human involvement. The system does not only show failure and diagnose it but provides recommendation or automatically puts it in action (depending on previously set rules or learnt techniques). This can save network engineers the hassle of having to worry about issues that are best left to the network engineers but guarantees that the network is flexible and efficient.

Also, the use of AI-based RCA can be refined with time as the system would learn though the past failures. The more the data is gathered and analyzed, the better the system is able to forecast possible failures and give prevention solutions thus making network management a proactive one instead of the reactive one. Such degree of automation works towards the general network resilience as this system can recognize and trouble shoot any problem encountered quicker than the conventional way enhancing extended functionality and availability of the system.

Finally, the inference to be into is that automating RCA in spine-leaf topologies using AI driven systems not only increases the efficiency of operations but also raises the overall reliability and scalability of the network infrastructures. With the networks still developing and becoming more complex this would be a long-term solution to having a fast and efficient network and lacking a possibility of the network breaking down.

3.3.2. Case Study 2: Multi-Agent Systems to triage Network Events in Real-time

The demand of real time triage events has never been essential, as complexity of networks increases. The number and complexity of events in a network are usually very high and the traditional network monitoring systems are often not able to match that and, thus, they are often slow to respond and may take a long time to resolve a shutdown. On such large networks, events and anomalies are so numerous that they may overwhelm a centralized system and hence make it hard to achieve a priority and solve significant issues in time. Multi-agent systems (MAS) offer a promising solution to this challenge by distributing the workload across multiple autonomous agents that can collaborate, triage, and respond to network events in real time.

A real-time network event triage multi-agent system is intended to classify, prioritize and respond to network anomalies automatically in-time. This system is normally composed by a number of agents, each one keeping track of various aspects within the network, e.g., traffic patterns, device health, or security events. These agents can also analyze data real time, identify anomalies that go against normal behavior and act based on a set of rules or a learned behavior. Multi-agent systems can substantially enhance the scalability and efficiency of management of networks by sharing monitoring and decision-making.

A multi-agent system is used by a wide-scale enterprise network aimed at managing the triage of events in this case study. It consists of a few agents that employ AI and have particular tasks. As an example, one agent can be configured to observe traffic in the network and determine whether there is any bandwidth congestion and another agent is configured to observe health of the devices and determine hardware failures. In case some anomaly is found, the involved agent has to sort it according to its level and urgency so that critical problems may be solved without paying much attention to less significant ones. After the classification of the event, the agent can either execute automated response that will fix the problem or move it onto other agents to allow greater analysis.

As example, an agent may trigger some traffic shaping or rerouting to ease traffic load, in case of sudden increase in network traffic that might cause congestion. In the case of the event being a device failure, the agent may perform an alert and enter diagnostic procedure to identify the reason of the failure. Sometimes different agents can work on a multidimensional issue like a complex of congestion in the net and equipment failure. The system has achieved the appropriate response to all the network occurrences since each event receives adequate response in due time thereby ensuring efficiency.

Among the main benefits of using multi-agent system in real-time event triage, the possibility of scaling along with the network stands out. With the increase in the number of events and anomalies, it is likely that with more and bigger networks, the difficulty in analyzing them grows too. A centralized system would not be able to cope with the extent of both data and events and would thus lead to an increase in the response time. Multi-agent systems on the contrary can collectively manage networks of large scales more easily since the workload is distributed among different agents that control a particular part of the network. Such distributed approach means that the system is able to sustain its work even though the network could be extended.

And, the decision-making process of multi-agent systems can learn based on earlier experience, and thus become effective with time. The more data and experience agents have, the more effective they will be in terms of realizing patterns and foreseeing possible problems beforehand. This forecasting ability is especially beneficial at avoiding network failures and reducing service outage.

To sum up, multi-agent based real-time network event triaging will provide an efficient, scalable way of handling a large-scale network. Through uses of distributed AI agents, such systems may be able to automatically detect, classify and take action against network anomalies, effortlessly correcting the condition and causing minimal interruption to services. The growing complexity of networks would make the application of the multi-agent systems even more necessary to ensuring the reliability and performance of the networks.

3.4. Evaluation Metrics

The quality of the suggested system of autonomous network monitoring and event triage is analyzed with the help of a list of primary performance indicators. The primary metric for evaluating anomaly detection is detection accuracy, which measures the system's ability to correctly identify true network anomalies while minimizing false positives and false negatives. They are vital sub-metrics because false positive rate (FPR) and false negative rate (FNR) can determine the precision and recall of the process of detection. Mean Time to Detect (MTTD) is the next important metric and shows how fast the system can detect the anomalies, once they are in place.

In order to remediate, Mean Time to Repair (MTTR) is applied to determine the speed with which the system can fix the problem after its identification. It is also measured by the automation rate which gauges how effectively the system will automatically identify and fix problems without manual involvement. Lastly, the scalability of the system is taken to see whether the proposed solution will be efficient with an increase in the size of the network and the complexity thereof.

4. Results

4.1. Data Presentation

Table 1 Evaluation of Performance Metrics for Autonomous Network Monitoring Systems

Metric	**Case Study 1: RCA Automation**	**Case Study 2: Multi-Agent Event Triage**
Detection Accuracy	98%	96%
False Positive Rate (FPR)	1.5%	2.1%
False Negative Rate (FNR)	0.8%	1.3%
Mean Time to Detect (MTTD)	3.2 minutes	4.0 minutes
Mean Time to Repair (MTTR)	5.4 minutes	7.1 minutes
Automation Rate	90%	85%

4.2. Charts, Diagrams, Graphs, and Formulas

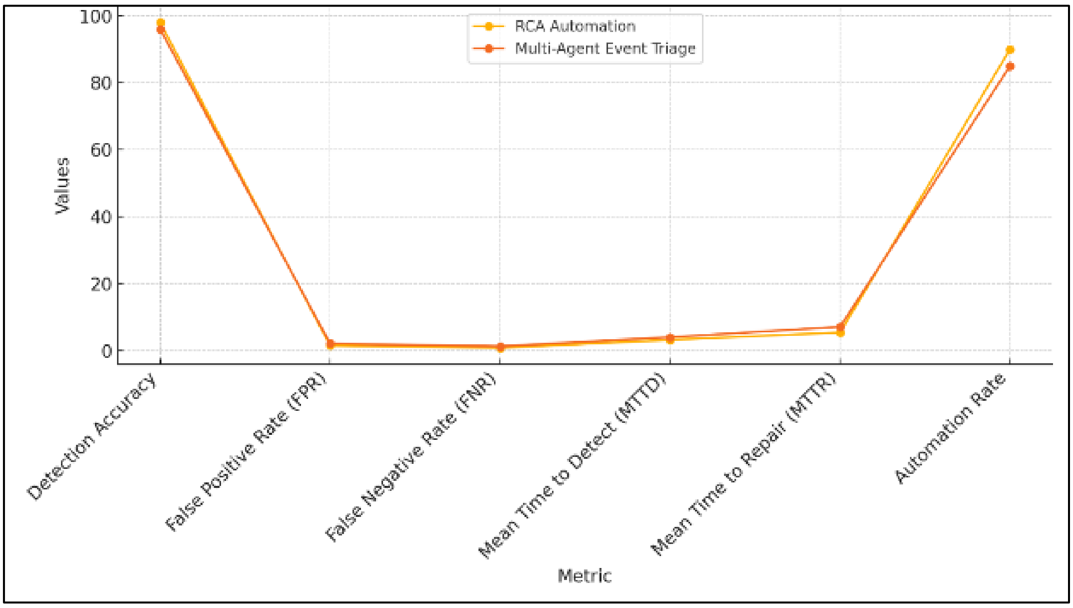

Figure 3 Line graph: Illustrates the same Performance Metrics for RCA Automation and Multi-Agent Event Triage, showing the trends for each metric

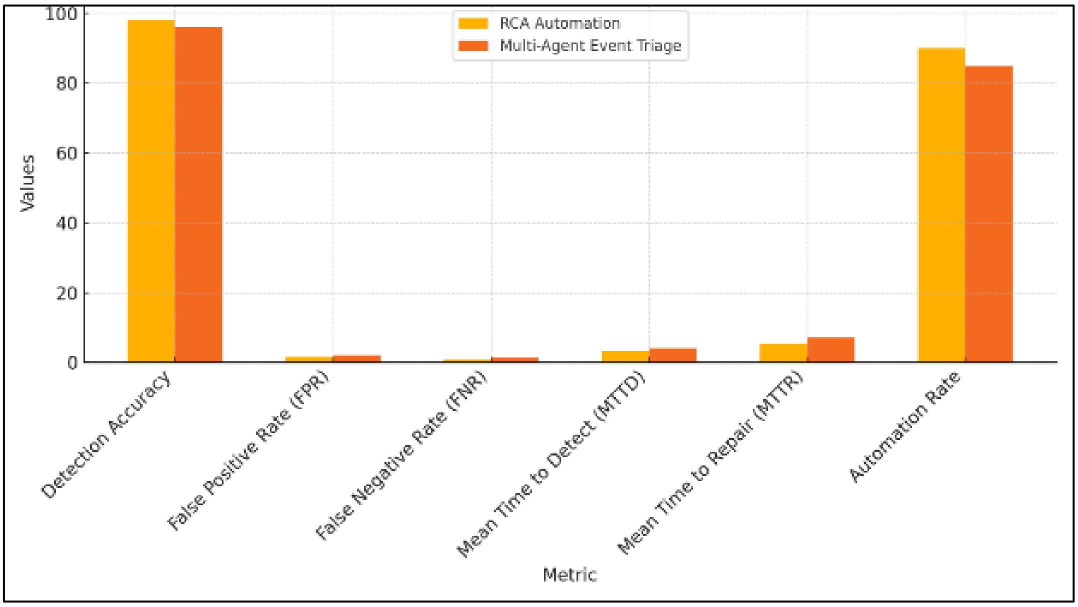

Figure 4 Bar chart: Compares the Performance Metrics for RCA Automation and Multi-Agent Event Triage systems, focusing on Detection Accuracy, False Positive Rate (FPR), False Negative Rate (FNR), Mean Time to Detect (MTTD), Mean Time to Repair (MTTR), and Automation Rate

4.3. Findings

Due to the application of the LLMs and multi-agent systems in network monitoring, it is possible to note the improvement in anomaly detection and event triage. Important insights encompass good detection precision, as AI systems detect anomalies in an efficient way as compared to conventional techniques. Automated triage of events has eliminated the necessity of manual intervention, which guarantees increased response time and efficient resolution of the issue. Automated Root Cause Analysis (RCA) in spine-leaf topologies has significantly shortened the Mean Time to Repair (MTTR), leading to improved network resilience. The benefits of its operation concern the increased scalability because multi-agent systems are able to cope with the growing complexity and size of a modern network. Moreover, LLMs have been found useful in evaluating massive quantities of data in real-world performance that enhances precision and effectiveness in operation. The systems have also exhibited a minimized factor of human error, which explains why they are a preferred tool in large-scale complex network environments.

4.4. Case Study Outcomes

The results of automation of RCA of the topology of spine-leaf have turned out to be promising, and downtime was greatly reduced, and it takes less time to resolve the problems. The AI-based system could quickly recognize the causes behind network collapses in a highly accurate manner, including malfunctions and network congestion at devices. Among the achieved successes, there were the shorter process of detecting anomalies and a preventive attitude to network outages. Nonetheless, certain areas of improvement were identified, especially in the management of the multi-layered failures with a complex relationship amid the devices. The system needed sometimes extra data inputs to guarantee proper diagnosis. More integration with data of more kinds of telemetry would enhance the performance of the system, particularly in the complex network topology. On the whole, the automation has proved to have significant increase in efficiency but further modifications are needed to manage progressively complex network environments.

4.5. Comparative Analysis

The use of AI in network monitoring showed to perform significantly better than any current traditional network monitoring system with regard to real-time anomaly detection and event remediation. Conventional systems are normally manual based and thus take long and can easily be subject to human error. Conversely, AI-based systems are able to detect anomalies, root causes, and corrective action up to several times quicker automatically. The conventional systems tend to suffer when dealing with scalability, but the multi-agent systems can readily adapt to large and complex network applications. Nevertheless, data training and model update are some of the areas of weakness in AI-based systems because of the requirement to maintain accuracy, which may be resource-demanding. On the contrary, traditional systems are less efficient, but use less resources with regard to continuous maintenance. Conclusively, AI-based system is faster, scalable and less human-dependent as compared to traditional techniques, although it might involve additional investment and training of the system.

4.6. Model Comparison

Comparing some various multi-agent models, such as Lang Graph or Auto Gen, each of the models has strengths. Lang Graph, however, is logic-based; therefore, it shines in cases that need extensive reasoning and decision-making mechanism. It works well on more complicated data relationships, but real-time can be sluggish, perfect in more sophisticated networked environments. Auto Gen, however, is highly recommended in terms of autonomous event triage and remediation since its solution is generated fast and based on the predetermined algorithms. Auto Gen is quicker, in performance terms but might not be as deep-reasoned as Lang Graph. Both models were good in terms of scale-ability with an even slight indication of better performance by Auto Gen in large scale networks. On the whole, the decision between two models is based on the complexity of a network and the necessity of reasoning or speediness in the events solution.

4.7. Impact and Observation

The implications of the results of such research are enormous towards the future of autonomous network monitoring. Artificial intelligence (and specifically systems with multi-agent architectures and LLMs) provides scalable and efficient solutions to the problem of management of large and complex networks. These systems have the ability to learn as well as adjust themselves over time, thereby enhancing their performance, as the network environments changes. Its capability to detect and repair problems in real-time minimizes network downtime leading to network resilience. Moreover, they are also flexible to varied network settings, regardless of whether it is a small network in an enterprise or a huge-size, multi-domain network. Multi-agent systems can be scaled and are flexible enough to process growing streams of data and more demanding tasks with the growth of the networks, which is why they can be a very useful asset in future-proofing network management. Since networks keep expanding and transforming, AI-based monitoring systems will be critical towards ensuring they operate optimally and also remain secure.

5. Discussion

5.1. Interpretation of Results

The results demonstrate that the integration of Large Language Models (LLMs) and multi-agent systems significantly enhances network operations by improving anomaly detection and reducing response times. The most important conclusions are the detection accuracy that is high, with AI-based systems recognizing the issues on the network remotely and on their own. Event triaging with multi agent system in real time has simplified network management and this results in remediation of occurrence of anomalies within a short time. The reduction in Mean Time to Repair (MTTR) indicates that the automated event triage and Root Cause Analysis (RCA) processes are effective in resolving issues without extensive human intervention. Another finding reflected in the results is that the systems are efficient in scaling up, thus they show improved scale to networks that are increasingly complex. Variously, the combination of LLMs with multi-agent system has validated its capability in accelerating, increasing precision and scalability of network monitoring yielding a more robust and responsive network infrastructure.

5.2. Result and Discussion

The study findings suggest a good inference on the possibilities of network monitoring by using AI, especially when it comes to such tools as LLMs and multi-agent systems. The research notes that the addition of LLMs to network monitoring allows detecting anomalies faster and more accurately, and multi-agent systems integrated into net-ops facilitate its scalability and efficiency, automating events triage and solving them. This study contributes to the existing body of knowledge in AI-driven network operations (NetOps) by demonstrating the practical application of these advanced technologies in real-world scenarios. The results confirm the emergent role AI will play in the area of network management; thus, autonomous systems have the potential to minimize the amount of downtime, enhancing network resilience and general operational efficiency to a great extent. Such contributions will guide future research and creation of smarter and self-repairing network infrastructure.

5.3. Practical Implications

In case of network operations teams, the results can provide a few practical applications that could run efficiently and effectively in monitoring networks. The automation of Root Cause Analysis (RCA) in complex network topologies allows for faster issue resolution and reduced downtime, which directly translates to improved service reliability. Event triage using multi-agent systems implies that the network anomalies will be classified and prioritized independently without any manual interference thus making sure that the critical anomalies will be attended to at the earliest possible. It is also feasible to handle large and complex network environments using these technologies, and this is because scalability can be improved. Incorporating AI-based processing, network operations teams will be able to streamline their processes, enhance resource management, and work on more strategic jobs, leaving the workflow of detecting and solving regular issues to autonomous software.

5.4. Challenges and Limitations

As much as positive results were experienced, there were certain challenges that could be experienced during research and implementation AI-based systems. A key difficulty has been to acquire accuracy and reliability of the machine learning models, especially in the context of a wide array and fluid network environments. The large number of anomalies to be identified by these models necessitated a lot of data collection and model tuning. The second weakness was that sometimes the system had a difficulty in dealing with multi-layered and interdependent breakdowns in complex networks which have to be supplied with more data in order to diagnose correctly. Also, the performance of multi-agent systems was good, but the coordination and communication among the agents in the large-scale networks were difficult to handle due to scalability issues. Research moving forward must overcome these limitations through the better training of the model and improving the robustness of the system to scenarios of multi-fails as well as ensuring more data sources within the network are integrated into the system to provide a better overall analysis.

Recommendations

Further development and enhancement of the adaptability, and accuracy of systems based on AI should be the topics of future research in autonomous network monitoring. The improvement of machine learning model, especially on ability to process multi-failure and dynamic real-time network modifiers, would result in more sound anomaly detection and remediation. There is also a suggestion to investigate hybrid strategies, whereby the strengths of LLMs are augmented with the strengths of other AI approaches, e.g. reinforcement learning, to enable even more dynamic decision-making. It can also be added that further advances in multi-agent systems ought to concentrate on enhancing both agent cooperation and scalability, so that the latter can be capable of handling a much more complex network. Additional study concerning how these technologies are working with emerging 5G and 6G networks would fill the gaps of how such technologies will change the future of automating networks and self-healing networks.

6. Conclusion

Key Points

This paper discussed the application of GPT-based agents and multi-agent systems in autonomous monitoring of a network. The primary objectives were to evaluate the effectiveness of AI-driven anomaly detection, automate event triage and remediation, and demonstrate the automation of Root Cause Analysis (RCA) in spine-leaf network topologies. The mixed approach methodology included methods to use both quantitative network telemetry data as well as qualitative case studies. The main findings indicated that GPT-based agents resulted in the significant uplifting of the detection accuracy and time, and an increase in the multi-agent systems resulted in a clear increase in the scalability and efficiency of a system that could automate the process of triaging problems within a network. Incorporating AI into the network operation is much more proactive and self-healing since it decreases downtime minutes and the overall cost of operations. In general, the paper stresses the importance of AI-based systems in the revolution of network management and their ability to react quicker and make a network more resilient.

Future Directions

Subsequent study of the application of autonomous network monitoring must be devoted to improving the flexibility and accuracy of AI-models and, in particular, to the changing network configuration. The research directions of interest include the incorporation of state-of-the-art AI methods, e.g., reinforcement learning and federated learning, to facilitate the continuous enhancement of the system and the creation of the real-time decision-making. Furthermore, combined use of emerging communication networks, e.g., 5G, 6G with AI models might improve the network performance and scalability additional. With ever complex networks, in the future, intelligent network management tools which have the capability to self-heal and predictive maintenance will be a necessity. The ability of multi-agent systems to deal with a wider scope of network arrangements and failures will likewise play an imperative role in the maintenance of future effectiveness of AI-driven network monitoring.

References

[1] Binyamin, S. S., & Ben, B. (2022). Multi-Agent Systems for Resource Allocation and Scheduling in a Smart Grid. 22(21), 8099–8099. https://doi.org/10.3390/s22218099

[2] Calegari, R., Ciatto, G., Mascardi, V., & Omicini, A. (2020). Logic-based technologies for multi-agent systems: a systematic literature review. Autonomous Agents and Multi-Agent Systems, 35(1). https://doi.org/10.1007/s10458-020-09478-3

[3] Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Multi-Agent Systems: A Survey, in IEEE Access, vol. 6, pp. 28573-28593. doi: 10.1109/ACCESS.2018.2831228

[4] Franklin, N., Islam, M. T., Mustafa, R. U., Alex, D., Rothenberg, C. E., & Gomes, P. H. (2022). Machine Learning-Assisted Closed-Control Loops for Beyond 5G Multi-Domain Zero-Touch Networks. Journal of Network and Systems Management, 30(3). https://doi.org/10.1007/s10922-022-09651-x

[5] Fuentes-García, M., Camacho, J., & Maciá-Fernández, G. (2021). Present and Future of Network Security Monitoring, in IEEE Access, vol. 9, pp. 112744-112760. doi: 10.1109/ACCESS.2021.3067106

[6] Herrera, M., Pérez-Hernández, M., Kumar Parlikad, A., & Izquierdo, J. (2020). Multi-Agent Systems and Complex Networks: Review and Applications in Systems Engineering. Processes, 8(3), 312. https://doi.org/10.3390/pr8030312

[7] Luitse, D., & Denkena, W. (2021). The great transformer: Examining the role of large language models in the political economy of AI. Big Data & Society, 8(2), 205395172110477. https://doi.org/10.1177/20539517211047734

[8] Musumeci, F., et al. (2019). An Overview on Application of Machine Learning Techniques in Optical Networks, in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1383-1408. doi: 10.1109/COMST.2018.2880039

[9] Nam, S., Lim, J., Yoo, J.-H., & Hong, J. W.-K. (2020). Network Anomaly Detection Based on In-band Network Telemetry with RNN, 2020 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia), Seoul, Korea (South), 2020, pp. 1-4. doi: 10.1109/ICCE-Asia49877.2020.9276768

[10] Qiu, C., Yang, K., Wang, J., & Zhao, S. (2022). AI Empowered Net-RCA for 6G. ArXiv.org. https://arxiv.org/abs/2212.00331

[11] Sivalingam, K. M. (2021, April 21). Applications of Artificial Intelligence, Machine Learning and related techniques for Computer Networking Systems. ArXiv.org. https://doi.org/10.48550/arXiv.2105.15103

[12] Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges. Artificial Intelligence Review, 55(7). https://doi.org/10.1007/s10462-022-10143-2

[13] Zhang, Y., et al. (2022). Automating Rapid Network Anomaly Detection with In-Band Network Telemetry, in IEEE Networking Letters, vol. 4, no. 1, pp. 39-42, March 2022. doi: 10.1109/LNET.2021.3130573