Author, 2026, 14:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Ai Agents For Autonomous Network Management: A Review Of Self-Monitoring, Self-Optimizing, Self-Healing And Self-Protecting Networks

Raskar Kasturi Ramesh[1] Prof. M. R. Kumbhoje[2] Prof. M. C. Kolse[3] Prof. S. K. Said[4]
Department of Artificial Intelligence and Data Science
Jaihind College of Engineering
Pune, Maharashtra, India

Abstract—Modern enterprise, cloud and mobile networks are large, complex and dynamic, and manual monitoring and configuration are slow, error-prone and unable to react quickly to failures, congestion and attacks. AI agents offer an intelligent approach in which software entities use machine learning, reasoning and automation to monitor, analyse and manage network operations with minimal human intervention. This paper reviews AI agents for autonomous network management. It traces the concept from the autonomic computing vision and its monitor–analyse–plan–execute loop, through software-defined networking and intent-based networking, to industry frameworks for zero-touch and autonomous networks. Machine learning techniques for traffic prediction, anomaly and fault detection, reinforcement learning for routing and resource management, graph neural networks for performance modelling, and language-model agents for configuration and troubleshooting are examined. Future directions such as 5G and 6G network automation, open radio access network controllers and network digital twins are discussed. A layered architecture with data collection, analytics, agent decision, orchestration and intent interfaces is proposed, together with research gaps, objectives, a comparison of techniques and a discussion of challenges including trust, safety of automated actions and data quality. The review concludes that AI agents can make networks more adaptive, reliable and secure while reducing operational cost.

Index Terms—AI agents, autonomous networks, network management, software-defined networking, intent-based networking, reinforcement learning, zero-touch automation, digital twin

I. INTRODUCTION

Networks today connect data centres, branch offices, cloud services, IoT devices and millions of mobile users. Configurations change frequently, traffic shifts by the hour and failures or attacks can cascade within seconds. Human operators, working through command-line interfaces and dashboards, struggle to keep pace, and many outages are caused by configuration mistakes.

The vision of self-managing systems was articulated by Kephart and Chess [1] in the form of autonomic computing, in which systems configure, optimize, heal and protect themselves according to high-level goals set by administrators. Two decades later, programmable networks and machine learning have made this vision practical for networking. Boutaba *et al.* [2] surveyed ML for networking and identified traffic prediction, classification, routing, congestion control, resource management, fault management and security as key areas.

This paper reviews AI agents for autonomous network management, proposes a layered architecture and discusses the obstacles to fully autonomous operation.

II. Background and Fundamental Concepts

A. The MAPE-K Loop

Autonomic management follows a closed loop of Monitor, Analyse, Plan and Execute over a shared Knowledge base (MAPE-K) [1]. An AI agent implements this loop: it observes the network, interprets the observations, decides on actions and applies them, learning from the results.

B. Self- Properties*

Fig. 1 summarizes the four self-* properties of autonomous networks: self-configuration, self-

© 2026 Author, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

optimization, self-healing and self-protection, together with the AI techniques that support each.

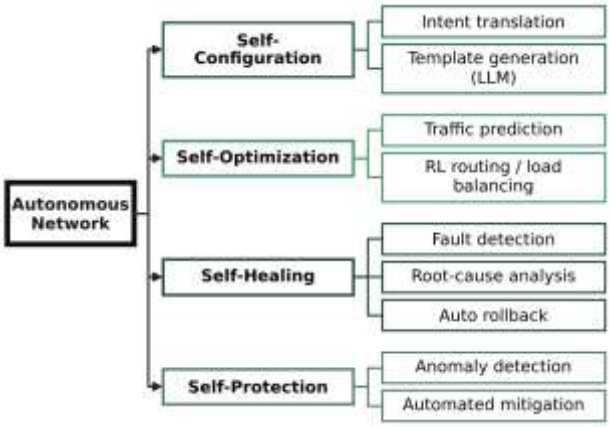


Fig. 1. Self-* properties of autonomous networks and supporting AI techniques.

II. ENABLING TECHNOLOGIES

Software-defined networking (SDN) separates the control plane from the data plane and exposes programmable interfaces such as OpenFlow [3], allowing agents to change forwarding behaviour through software [4]. Intent-based networking [5] lets operators express desired outcomes rather than device-level commands. The ETSI zero-touch network and service management framework [6] defines an architecture for end-to-end automation.

III. LITERATURE SURVEY

Kreutz *et al.* [4] provided a comprehensive survey of SDN, explaining how centralized controllers and open interfaces make network behaviour programmable, a prerequisite for AI-driven management. Boutaba *et al.* [2] reviewed ML across networking problems and noted that data availability and generalization across networks are major challenges.

Reinforcement learning (RL) has been used for control decisions. Mao *et al.* [7] showed that a deep RL agent can learn resource scheduling policies that outperform heuristics, and Pensieve [8] used RL to adapt video bit rates to network conditions, improving user experience. Valadarsky *et al.* [9] explored learning to route, training agents to choose routing configurations that perform well across changing traffic demands.

For performance modelling, RouteNet [10] used graph neural networks to predict delay and jitter for any topology and routing configuration, allowing an agent to evaluate candidate changes before applying them, a capability closely related to network digital twins.

For security and fault detection, Kitsune [11] demonstrated online unsupervised anomaly detection with autoencoder ensembles that run on modest hardware. In mobile networks, Polese *et al.* [12] described the open radio access network (O-RAN) architecture, whose RAN intelligent controllers host AI applications that optimize radio resources in near real time. Saad *et al.* [13] envisioned 6G networks in which AI is native to network operation. More recently, language-model agents that reason and act with tools [14] have been explored for translating intents into configurations and assisting troubleshooting. Table I summarizes these works.

Sr. No.	Ref.	Year	Methodology	Findings	Research Gap
1	[1]	2003	Autonomic computing vision (MAPE-K)	Defined self-managing system properties	Conceptual; no network specifics
2	[4]	2015	Survey of software-defined networking	Programmable control enabling automation	Controller scalability concerns
3	[7]	2016	Deep RL resource management	Learned policies beat heuristics	Simulated environment
4	[9]	2017	Learning to route	RL routing robust to demand changes	Small-scale evaluation
5	[2]	2018	Survey of ML for networking	Mapped ML to networking tasks	Generalization challenges noted
6	[11]	2018	Kitsune online anomaly detection	Unsupervised real-time intrusion detection	Sensitive to training contamination

Sr. No.	Ref.	Year	Methodology	Findings	Research Gap
7	[10]	2020	RouteNet graph neural network	Accurate delay prediction for any topology	Training data generation cost
8	[5]	2022	Intent-based networking concepts	Outcome-driven network management	Implementation guidance limited
9	[12]	2023	O-RAN architecture survey	AI apps in RAN intelligent controllers	Security and interoperability issues

TABLE I Summary of Literature Survey

IV. RESEARCH GAP

The following gaps are identified:

- **G1:** Most AI models are evaluated in simulation or on a single network and generalize poorly to other topologies and traffic.
- **G2:** Safety guarantees for automated actions are limited; a wrong action can cause widespread outages.
- **G3:** Explaining agent decisions to network operators is rarely addressed.
- **G4:** Coordination among multiple agents managing different domains can lead to conflicting actions.
- **G5:** Validating LLM-generated configurations before deployment remains an open problem.

V. OBJECTIVES

The objectives of this review are:

• To study the concepts of autonomic and autonomous network management.

• To review AI techniques for monitoring, optimization, healing and protection of networks.

• To propose a layered AI-agent architecture for autonomous network management.

• To compare techniques in terms of capability, data needs and maturity.

• To discuss challenges and future developments such as 6G, digital twins and generative AI.

VI. PROPOSED SYSTEM ARCHITECTURE

Fig. 2 shows the proposed architecture, which implements the MAPE-K loop with specialized agents and a digital twin for safe validation.

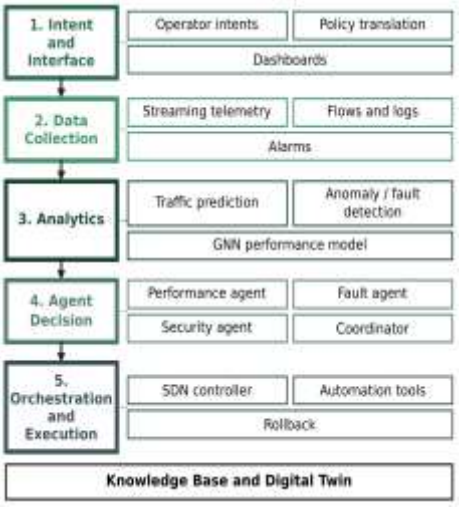


Fig. 2. Proposed AI-agent architecture for autonomous network management.

1. Intent And Interface Layer

Operators state objectives such as "keep video latency below fifty milliseconds" or "isolate infected hosts," through dashboards or natural-language interfaces. Intents are translated into measurable policies.

2. Data Collection Layer

Streaming telemetry, flow records, logs, alarms and configuration states are gathered from routers, switches, controllers and radio units.

3. Analytics Layer

ML models predict traffic, detect anomalies, localize faults and assess security threats. A graph-based performance model estimates the effect of possible changes.

4. Agent Decision Layer

Specialized agents for performance, fault and security plan actions. A coordinator resolves conflicts between agents. Candidate actions are tested on a network digital twin before approval.

5. Orchestration And Execution Layer

Approved actions are applied through SDN controllers and automation tools, and results are monitored; if outcomes worsen, changes are rolled back automatically.

VII. METHODOLOGY AND WORKING

The control loop is shown in Fig. 3. An RL agent observes state s_t, takes action a_t and receives reward r_t; it learns a policy that maximizes the expected discounted return

$$G = \Sigma_t \gamma^t \cdot r_t \qquad (1)$$

where γ is a discount factor between zero and one. A reward for traffic engineering may combine throughput, latency and link utilization, for example

$$r = \alpha \cdot Throughput - \beta \cdot Latency - \lambda \cdot max(Utilization) \qquad (2)$$

Anomalies are flagged when a model's reconstruction or prediction error exceeds a learned threshold.

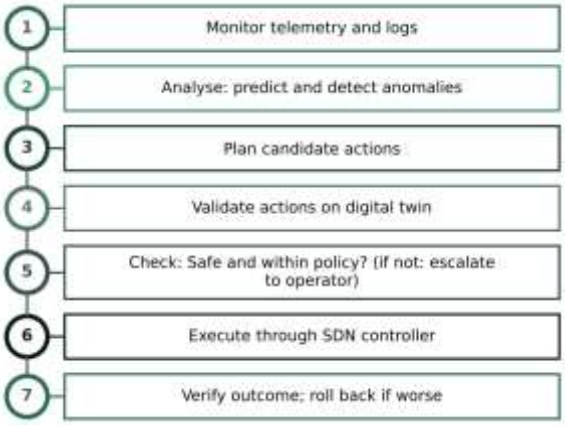


Fig. 3. Closed-loop (MAPE-K) workflow of the AI network agent.

Network availability, mean time to detect, mean time to repair and the proportion of incidents resolved without human intervention are used to evaluate the system.

VIII. COMPARATIVE ANALYSIS

Table II compares AI techniques for network management. Supervised and unsupervised ML are mature for prediction and anomaly detection; RL is powerful for control but risky without safeguards; GNNs model topology-dependent performance; and LLM agents are promising for intent translation but need validation.

Technique	Use	Maturity	Risk
Supervised ML	Traffic / fault prediction	High	Low
Unsupervised ML	Anomaly detection	High	Low–Medium
Reinforcement learning	Routing, resources	Medium	High
Graph neural networks	Performance modelling	Medium	Low
LLM agents	Intent, config, troubleshooting	Emerging	Medium–High

TABLE II Comparison of AI Techniques for Network Management

IX. CHALLENGES AND FUTURE SCOPE

Table III summarizes the main challenges. Future developments include fully zero-touch operation in 5G and 6G networks, AI-native radio controllers, high-fidelity digital twins for what-if analysis, generative AI assistants that write and verify configurations, and standards for interoperable agents across vendors and domains.

Challenge	Mitigation
Unsafe automated actions	Digital-twin validation; auto rollback
Poor generalization	Transfer learning; diverse training data
Operator trust	Explanations; human approval for high impact
Agent conflicts	Central coordinator; policy priorities
Data quality	Telemetry standards; data validation

TABLE III Challenges and Mitigation

X. CONCLUSION

AI agents are bringing the long-standing vision of autonomic networking into practice. The reviewed literature shows that ML can predict traffic and detect anomalies, RL can learn effective control policies, GNNs can model network performance and programmable

infrastructures allow agents to act. A layered architecture with intents, analytics, coordinated agents, digital-twin validation and automatic rollback can deliver self-monitoring, self-optimizing, self-healing and self-protecting networks. Trust, safety and explainability must be addressed so that operators can confidently delegate control to AI agents.

1. Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

REFERENCES

1. J. O. Kephart and D. M. Chess, "The vision of autonomic computing," Computer, vol. 36, no. 1, pp. 41–50, 2003.
2. R. Boutaba et al., "A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities," J. Internet Serv. Appl., vol. 9, Art. no. 16, 2018.
3. N. McKeown et al., "OpenFlow: Enabling innovation in campus networks," ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008.
4. D. Kreutz et al., "Software-defined networking: A comprehensive survey," Proc. IEEE, vol. 103, no. 1, pp. 14–76, 2015.
5. A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, "Intent-based networking—Concepts and definitions," IETF RFC 9315, 2022.
6. ETSI, "Zero-touch network and Service Management (ZSM); Reference architecture," ETSI GS ZSM 002, 2019.
7. H. Mao, M. Alizadeh, I. Menache, and S. Kandula, "Resource management with deep reinforcement learning," in Proc. 15th ACM Workshop Hot Topics Netw. (HotNets), 2016, pp. 50–56.
8. H. Mao, R. Netravali, and M. Alizadeh, "Neural adaptive video streaming with Pensieve," in Proc. ACM SIGCOMM, 2017, pp. 197–210.
9. A. Valadarsky, M. Schapira, D. Shahaf, and A. Tamar, "Learning to route," in Proc. 16th ACM HotNets, 2017, pp. 185–191.
10. K. Rusek et al., "RouteNet: Leveraging graph neural networks for network modeling and optimization in SDN," IEEE J. Sel. Areas Commun., vol. 38, no. 10, pp. 2260–2270, 2020.
11. Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Proc. Netw. Distrib. Syst. Security Symp. (NDSS), 2018.
12. M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," IEEE Commun. Surveys Tuts., vol. 25, no. 2, pp. 1376–1411, 2023.
13. W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Netw., vol. 34, no. 3, pp. 134–142, 2020.
14. S. Yao et al., "ReAct: Synergizing reasoning and acting in language models," in Proc. Int. Conf. Learn. Represent. (ICLR), 2023.