Autonomous Network Research

1. Fundamentals Of Networks
2. Connectivity and Infrastructure
3. Emerging Technologies
4. Network Management (Autonomous VS. Non-Autonomous)
5. What is an Autonomous Network?
6. The Autonomous Network Framework (ANF) IG1218F
7. The Autonomous Network Architecture

1 Fundamentals of Networks

A network in the context of telecommunications serves as the system that enables devices to communicate with each other.

1.1 Components of a Network

There are a number of major components which build a network system:

First, are the devices (called nodes) which can be computers, TVs, smartphones, servers, etc.

Second, there are protocols which are the rules that dictate that manner by which data is transmitted across the network. Protocols can be thought of as the languages devices must speak in order to understand each other. TO ADD: What is the protocol being used at VodafoneZiggo in the context of this project (IP/TCP)?

Commented [EC1]: TCP/IP: on the internet. Will add more detailed info later
HTTP/HTTPS
FTP: used to transfer files between systems.

Thirdly, there are the connections between the devices (nodes) known as links. These can be physical cables (e.g., fiber) or wireless connections (e.g., Bluetooth, Wi-Fi). (Ethernet cables that connect computers to routers, fiber optic cables delivering internet, or wireless signals from a Wi-Fi router).

Forth, there is the data, which is the information being transmitted across the network system (text messages, emails, files, etc.).

Fifth, are the switches and routers which control the data flow. Switches are the devices that connect multiple nodes within a LAN, and make sure that the data gets to the correct device within the local network. Routers are the devices that direct data between different networks. (e.g., a home router is responsible for sending data between the local network and the internet).

1.2 Types of Networks

Wireless Networks are networks without no physical cables, by which devices communicate over radio signals.

In addition, Local Area Networks (WAN) covers large areas like cities or countries (e.g., the internet). Their purpose is to connect distant networks together to allow for communication across cities, counties, or even the entire globe.

Further, Local Area Networks (LAN) covers a small area, like an office or home. They allow users to share resources (for example a printer), and access the internet through a single connection.

Last, Metropolitan Area Network (MAN) is a large network that covers a large space, often connecting several LANs. Their purpose is to serve a larger geographical are than LANs but smaller than WANs, and to provide efficient communication for organizations spread across a city or region (e.g., a network that connects different departments or buildings in a university campus).

1.3 Key Concepts in Networking

There a number of frequently used concepts in networking which are important to know about.

Bandwidth: refers to the maximum amount of data that can be transmitted over a network in a given amount of time. Higher bandwidth connection allow for faster internet speeds and the ability to handle more devices or applications (like streaming a video or gaming)

Latency: refers to the delay between sending a request and receiving a response over the network. Low latency is important for real-time applications like gaming, video conferencing, or controlling IoT devices.

2 Connectivity and Infrastructure

2.1 Fiber vs Coax

Fiber uses light to transmit data through glass or plastic cables. It offers faster speeds and greater capacity, suitable for long distances with minimal signal loss.

On the other hand, Coax uses electrical signals over copper cables, commonly used for cable TV and broadband internet. Its slower than fiber and more susceptible to interference. Coax is often used in older internet infrastructure, delivering moderate speeds but with more limitations over distance.

2.2 Fixed Networks

Fixed networks are wired networks (fiber, DSL, cable), that provide stable, high-speed internet to stationary locations such as homes and offices. A fixed fiber connection in a home provides consistent, high-speed internet compared to mobile networks that rely on cell towers.

3 Emerging Technologies

3.1 5G

5G or The 5th Generation of mobile network technology, providing much faster speeds, lower latency, and the ability to connect many devices simultaneously. For example, 5G enables real-time data transmission for autonomous cars, allowing them to communicate with each other and avoid collisions.

3.2 The Internet of Things (IoT)

IoT refers to billions of connected devices that collect and share data over the internet, from home appliances to industrial machinery. Smart thermostats, security cameras, and fitness trackers that collect and send data to apps on your phone.

3.3 Why the Incorporation of 5G and IoT Increase Network Complexity

The reason behind why new emerging technologies are causing network complexity is mainly due to increased devices and traffic. 5G enables millions of IoT devices to be connected simultaneously, creating more traffic and requiring smarter network management.

4 Network Management

Management in the context of network management refers to the process of ongoing monitoring, controlling, and maintenance of the performance of the network.

4.1 Non-Autonomous Network Management

Involves work by employees such as administrators and network engineers. They key tasks of these employees include the following:

1. Network Configuration: configuring network devices (e.g., routers, switches) in an optimized way based on the needs of the network. This may include, for example, prioritizing certain types of network traffics or setting bandwidth limits.
2. Monitoring: using tools/software to monitor the status of the network. The monitoring can either be in the means of fixing issues “on the spot” (i.e., as they occur), or by means of identifying potential issues before they occur.
3. Troubleshooting: this entails the diagnostic process of issues that have occurred (e.g., security attacks, misconfiguration, hardware problems, etc.), by means of

manually reviewing system logs and running tests in hopes of identifying the root causes of the issues.

4. Maintenance: manually handling regular updates to security, software and hardware in the effort to ensure that everything is running efficiently.

4.1.1 Challenges of Non-Autonomous Network Management

There are a number of potential issues that arise when the traditional non-autonomous network management paradigm is used.

The most obvious issue is the likelihood of human error. Like all manual processes, manual network management is prone to mistakes that can cause security issues or network outages if some misconfigurations or other faulty tasks are overlooked.

Another challenge of the traditional management paradigm is scalability. As networks grow in their complexity and breadth, it become increasingly challenging and more resource-intensive to manage the network. In other words, as the scale of the network grows, the number of employees required to monitor and manage it grows as well.

Finally, when problems in the network occur it can be time consuming to troubleshoot and fix issues when done manually. Troubleshooting can be extremely slow if the network is complex, and, as a result, can create a lot of frustration in both employees as well as with customers.

4.2 Autonomous Network Management

Autonomous network management (ANM) employs Artificial Intelligence and Machine Learning tools to automate the management of networks, with minimal to no human intervention. The key features of the autonomous network management paradigm can be identified as the following:

1. Self-Monitorization: AI-powered systems can monitor the network continuously and in real-time, without requiring constant human supervision.
2. Self-Healing and Self-Troubleshooting: When problems with the network arise, the autonomous networks can automatically diagnose the underlying cause, and the network will try to recover from failures or repair them on its own. (e.g., a router fails. The network then re-routs traffic through alternative paths to maintain continuous network service).
3. Self-Optimization: the incorporation of AI tools allows to analyze network performance over time, learning from patterns and making adjustments to improve efficiency. (e.g., ensuring efficient utilization of resources, optimization of data paths, etc.)

Commented [G(2]: This is a nice part. This can help us to structure the use cases we have, and the new use cases to know in which are they help us to move towards a level 4/5 of AN.
Maybe a nice idea is to have a slide on this, so we can use when you meet people to give you more information about the network, then for the use cases they have you can have a discussion on where do they fit.

4. Self-Securing: the ability to automatically detect and respond to anomalies relating to security threats, and respond to them in real-time. AI-based intrusion detection systems can analyze traffic patterns and block or isolate suspicious activities to protect the network from cyberattacks.
5. Self-Configuration: the ability to self-configure based on network conditions. (e.g., automatic adjustments to bandwidth for certain services). It also entails that the system will be able to configure new devices that are added to the network with minimal human input.

Commented [CE(3]: Comprehensive explanation and examples for future reference: https://www.sciencedirect.com/science/article/pii/S2665917423001630

4.2.1 Advantages of Autonomous Network Management

Advantage	Explanation	Example
Predictive maintenance	AI can detect potential problems before they become serious.	
Reduced human error	Automation reduces the chance of mistakes that might occur with non-autonomous management, as necessary configurations and adjustments are made based on algorithms that are precise.	A network engineer misconfigures a firewall, causing an outage. In an autonomous system, AI handles the configuration, which reduces the chance for mistake.
Efficiency and speed	AI can identify and mend problems much faster than humans, which in turn reduces downtime and minimizes the impact of issues in the network.	If a router in a network fails, an AI system can detect it immediately and re-route traffic in seconds, preventing noticeable downtime for customers.
Scalability	ANs can manage large-scale, complex environments more easily, as AI systems can handle vast amounts of data and adapt to changing conditions in real-time.	VodafoneZiggo adds hundreds of cell towers to its network. The autonomous system automatically integrates them and optimizes traffic without the need for manual intervention.
Cost efficiency	Reduces the need for large teams of administrators, which lowers operational costs.	VodafoneZiggo automates network management with AI, reducing the need for a large IT team to manually monitor and

		maintain the network, saving on labor costs.

4.2.2 Challenges of Autonomous Network Management

Although there are numerous advantages to embracing an ANM paradigm, there are still some challenges to be accounted for.

Firstly, is can result in some security risks, since AN can also open new surfaces for potential attacks. If the system is compromised, it might be a challenge to detect it or stop it quickly.

Second, there are some high costs that are entailed within the process of setting-up an AN, as it requires investment in AI and automation technologies.

Last, it can be complex to both develop and maintain the AI systems that run the ANs.

5 What is an Autonomous Network?

An Autonomous Network (AN) is a self-managing network that leverages Artificial Intelligence (AI), Machine Learning (ML), and automation technologies to perform various tasks without human intervention. These tasks include self-configuration, self-optimization, self-healing, and self-protection. The aim of AN is to handle network operations dynamically and efficiently, optimizing performance in real-time based on the constantly changing state of network.

5.1 TM Forum's Definition of Autonomous Networks

According to TM Forum's IGI1218F (p.6), autonomous networks are designed to achieve zero-touch operation, which means that the system should operate without the need for manual configuration or intervention from human operators. Instead, AI and closed-loop automation continuously monitor the network, analyze data, and execute decisions such as re-routing traffic or adjusting bandwidth allocation.

In the TM's Forum's framework, zero-touch, zero-wait, zero-trouble are the core goals of ANs. There refer to:

- Zero-Touch: the network should autonomously handle routine tasks.
- Zero-Wait: Real-time, immediate responses to network demands.
- Zero-Trouble: Self-healing and self-protective mechanisms that prevent network issues from affecting customers.

The role of AI in this context is critical, as the network relies on ML algorithms and real-time data analytics to predict and preemptively solve issues, ensuring seamless operation even as demand change. The AI in AN relies on several types of machine learning techniques:

1. Supervised Learning: This involves training AI models using historical labeled data to predict and optimize network behavior. For example, a model might predict traffic congestion based on previous patterns, allowing the network to re-route traffic preemptively.
2. Reinforcement learning: In this type of learning, the AI learn by interacting with the network environment. It receives feedback (rewards or penalties) based on its actions, helping in optimize decisions over time. This is especially useful for adjusting traffic routing in response to real-time network conditions.

Commented [EC4]: Source: "Landing AI on Networks: An equipment vendor viewpoint on Autonomous Driving Networks"

5.2 AI Driven Self-X Capabilities

ANs possess self-X capabilities, a term used to describe the various self-managing function the network can perform autonomously. These include:

1. Self-Configuration: the ability to automatically configure network devices such as routers, switches, and virtual machines based on predefined goals.
2. Self-Optimization: Continuous adjustments of network parameters to optimize performance metrics, such as latency and energy efficiency.
3. Self-healing: The network's ability to detect and mitigate security threats in real time.
4. Self-protection: The capability to autonomously detect and mitigate security threats in real time. This can be done by using unsupervised learning models that identify anomalous behavior in traffic, such as DDoS attacks.

Commented [EC5]: Source: "Exploring unsupervised Learning with Clustering and Autoencoder to Detect DDoS attack"

Each of these function is powered by AI-driven automation, which guided by the analysis of data streams from network devices and traffic. For instance, in self-healing, the AI identifies performance anomalies (e.g., failing server) and autonomously takes corrective actions, such as re-routing traffic or restarting the server to minimize downtime.

6 The Autonomous Network Framework (ANF) IG1218F

This section covers key insights from the IGI1218F document, providing a comprehensive understanding of the framework needed to build and implement AN in a telecommunications environment. The content in relevant for progressing toward automated network management within VodafoneZiggo.

6.1 Key Elements of ANF

There are 4 relatively independent key elements of ANF.

1. Key Effectiveness Indicators (KEIs): helps to determine the benefits of enhancing the telecommunications systems with greater autonomy capabilities.
2. Autonomous Network Levels (AN Levels): The framework establishes six levels of network autonomy, which offer a clear progression pathway toward full network autonomy.
   - L0 (Manual): all network operations are manually managed.
   - L1 (Assisted): automation handles repetitive tasks, but critical decisions remain manual.
   - L2 (Partial Autonomous): automated systems perform predefined tasks based on rules.
   - L3 (Conditional Autonomous): the network can adapt to real-time changes without human assistance.
   - L4 (Highly Autonomous): AI-driven, the network predicts issues and resolves them proactively.
   - L5 (Fully Autonomous): End-to-end automation with minimal to no human intervention.

3. AN Target Architecture: (detailed in the next section).

4. AN Map: This is a roadmap for CSPs to prioritize what areas of the network to automate first.

- Service-oriented: focuses on improving customer-facing services.

- Network-oriented: focuses on automating the physical network (routers, switches, etc).

Commented [CE(6]: This is where we are (if I remember correctly)

Commented [G(7R6]: Correct, we are somewhere between 1 and 3, for some parts we are 1 and some parts maybe 2 or 3.

Commented [CE(8]: This is where we want to be in the near future (if I remember correctly)

Commented [G(9R8]: Yes, the aim is between 4 and 5.

Commented [EC10]: Was there a choice made already in this regard? Or are we free to choose?

Commented [G(11R10]: Not sure about this, we probably need to ask Arjan Eeken - he was busy with the Automation roadmap for Fixed Network. Would be nice to have a talk with him. I also know that the GenAI squad is algo thinking about the AN concept but they don't have the network knowledge, so we should take charge of which areas to start, together with them for the feasibility, but we should make a plan on this. (we I mean Technology)

6.1.1 AN L3/L4 Characteristics

"There is now industry consensus that AN Levels are defined based on cognitive closed-loop theory and the degrees of a human-machine division of labor."

6.1.1.1 Cognitive Closed-Loop Theory

This theory refers to a system where feedback from the network (like data on performance or issues) is constantly being processed, and actions are automatically taken to address or improve the situation. The "cognitive" aspect means that the network isn't just reacting to issues but learning from then over time to predict and prevent problems before they arise.

In essence, the network becomes smarter as it operates, and decisions are made automatically in a loop of monitoring, feedback, and adjustment. This closed-loop process enables the network to evolve its operations without human intervention, a critical feature in reaching higher levels of autonomy.

Academic sources discuss the importance of feedback-driven decision making in both AI and autonomous systems, highlighting that this feedback loop is essential for enabling networks to adjust and self-optimize over timer, as seen in autonomous systems like self-driving cars and other AI-managed environments.

Commented [EC12]: Source 1: https://link.springer.com/article/10.1007/s10111-020-00637-w

Source 2: https://ieeexplore.ieee.org/document/9904673

6.1.1.2 Human-Machine Division of Labor:

As networks become more autonomous, the division of tasks between humans and machines shifts. At lower level autonomy (L0-L1), humans make most decisions, and the network only assists with repetitive or basic tasks. As you progress to higher levels (L3-L4), the network can handle more complex tasks, such as self-optimization and predictive maintenance, with little to no human intervention.

The division of labor aspect is key to understanding how much control is handed over to the network. At the highest level (L5), the network operates fully autonomously, requiring no human input, except in extraordinary circumstances.

In academic research, the idea is often referred to as human-autonomy teaming (HAT), where both the human and machine share responsibilities, but the machine takes over on more complex and autonomous decision-making roles as it becomes more capable.

Commented [EC13]: Source 1: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.589585/full

Source 2: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9284085/

7 The Autonomous Network Architecture

The Autonomous Network Architecture Technical Architecture, as described in GI1230, defines a layered, modular structure that allows the network to be self-governing, adaptive, and scalable. It shows the integration of AI, Network Function Visualization (NFV), Software-Defined Networking (SDN), and intent-driven interactions. The architecture enables closed-loop automation and fosters autonomous decision-making through distributed intelligence. Below, I will break down the key components of the AN architecture and their interplay.

7.1 Autonomous Networks Technical Architecture: Layered Model

The AN architecture is stratified into three major layers, each responsible for managing different aspects of network operations.

1. Resource Operations Layer: this layer is responsible for managing the physical and virtual resources of the network, such as routers, switches, and servers. The resource operation layer works with virtualization technologies like NFV and SDN to provide a flexible and programmable network infrastructure. This layer

interacts closely with the service operations layer to ensure that the network resources align with service-level requirements.

2. Service Operations Layer: the service operations layer focuses on *service orchestration* and optimization. This layer ensures that all services meet their *service-level-agreements (SLAs)*. Ai-driven service orchestration tools monitor the network in real-time, ensuring that services are delivered efficiently and optimized based on demand.
3. Business Operations Layer: the business operations layer aligns network performance with business goals, such as maximizing customer satisfaction, reducing operational costs, or increasing profitability. The AI-driven *decision engines* in this layer ensure that network services and operations are aligned with the company's broader objectives.

7.1 Autonomous Domains and Intent-Driven Interactions

One of the core concepts of the AN technical architecture is the division of the network into Autonomous Domains (ADs). These domains are self-contained units that manage specific network functionalities and are governed by a set of policies and rules that dictate their autonomy.

AD communicate through *intent-driven interfaces*, a high-level abstraction model where network operators express desired outcomes which are then translated by the AI system into network actions.

Each AD operates independently but cooperates with other domains to deliver end-to-end services (cross-domain integration). ADs encapsulate various network operations, such as routing, traffic management, and security, while optimizing these based on real-time analysis and intent.

7.1.1 Intent-Based and Zero-Touch Operations

Intent-Based Networking (IBN) plays a key role in autonomous networks by allowing operators to define high-level goals, known as intents, rather than configuring the network manually. These intents are abstract, meaning that operators do not need to specify the exact steps to achieve their goals. Instead, the network's AI translates these intents into actionable commands that align with the network's objectives, ensuring zero-touch operations where tasks are performed automatically without human involvement. IBN is closely tied to the closed-loop, since the closed-loop allows the network to constantly evaluate its performance against the defined intent.

For example, if an operator's intent is to "minimize latency for a particular service", the AI will dynamically adjust the network parameters and configurations to meet this goal by re-routing traffic or prioritizing resources. This capability is particularly important as

networks evolve towards L4 and L5 autonomy, where the system can fully execute and optimize tasks across multiple domains and services without human intervention.

7.1.2 Intent Handling

The AI system within an AN process high-level intents provided by network operators or users. These intents define goals that the network must achieve autonomously. The intent API facilitates communication between different layers and functions of the network and by ensuring the intents are translated into actions.

7.2 AI and Closed-Loop Automation

Closed-Loop automation is at the heart of ANs, allowing the network to continually optimize its operations by feeding real-time data back into AI models. This process is autonomous and ongoing, enabling the network to detect inefficiencies, faults, or potential risks and adjust configurations accordingly. For example, in response to unexpected surge in traffic, the network can automatically scale or adjust routing paths to balance the load, ensuring minimal disruption.

As noted in TM Forum's IG1230, closed-loop automation involves several stages: awareness, analysis, decision making, and execution of network optimization. AI systems are responsible for analyzing data from various network components, predicting failures, and adjusting the network in real time. This process operates autonomously across multiple layers of the network, including both service and resource levels.

1. Awareness: In this stage, telemetry data from network elements (e.g., switches, routers) is collected in real-time, including metrics such as bandwidth, latency, and fault logs.
2. Analysis: AI models analyze this data to identify anomalies, optimize traffic, or detect potential failures. Techniques like ML are used to predict future network conditions.
3. Decision-Making: Based on the analysis, AI determines the optimal actions to take in order to maintain or improve network performance. This could include actions like re-routing traffic or allocating additional bandwidth.
4. Execution: The network implements these decisions automatically through its management systems, reconfiguring itself without human oversight.

7.3 Network Function Virtualization (NFV)

Commented [C(14]: Further explanation: What Is Network Functions Virtualization (NFV)? | IBM

Network Function Virtualization (NFV) *decouples* network functions from dedicated hardware devices and runs them as virtual instances on *standardized* hardware. This enables the network to dynamically instantiate or terminate network functions based on current demand, providing greater scalability and flexibility.

In AN, NFV allows the network to quickly deploy, and scale services based on real-time demand. For example, if traffic to a particular service increase, the network can instantiate additional virtual instances of network functions to handle the increased load.

7.4 Software-Defined Networking (SDN)

SDN is another foundational technology in AN, providing the programmability required for AI-driven decision making. SDN separates the *control panel* from the *data plane*, allowing network operators to control traffic flows programmatically through a centralized controller.

In AN, SDN enables real-time network adjustments by interacting with AI-driven decision engines. The centralized control plane provides a global view of the network, allowing the AI system to dynamically re-route traffic, allocate bandwidth, and optimize resources based on real-time data.

Commented [C(15]: Academic paper talking about SDN in IBN Intent-driven autonomous network and service management in future cellular networks: A structured literature review (arxiv.org)

Commented [C(16R15]: section 2.5

7.5 AN Target Architecture

The AN target architecture defines a holistic framework for the future of self-managing networks. By decomposing the network into Autonomous Domains (ADs) and integrating AI decision-making, closed-loop automation, and *intent-driven interfaces,* this architecture enables a fully autonomous, scalable, and adaptive network infrastructure. AI models, in combination with intent-based management and cross-domain collaboration, provide the tools necessary for achieving network autonomy.

7.5.1 Core Elements of the AN Target Architecture

The components of the AN target architecture work together to reduce complexity and by decomposing the network into Autonomous Domains (ADs).

1. Intent-Driven Interfaces: the architecture uses intent-based networking (IBN) to abstract operational goals from detailed configurations. Operators provide a high-level objective, which AI translates into specific technical actions. Intent is defined and executed autonomously through machine learning models embedded within the network.
2. Closed-Loop Automations: this is the core of the architecture- AI systems continuously monitor, analyze and adjust network behavior.

8 Knowledge and Intelligence in AN Technical Architecture

AI allows networks to analyze vast amounts of real-time data, predict network behavior, and autonomously adjust configurations.

8.1 AI Usage Modes

1. Development Mode (Sandbox): a sandbox is a controlled and isolated testing environment where AI models can be trained, tested, and validated before being deployed to a live network. This mode ensures that AI models are thoroughly evaluated without impacting the live system. In the context of ANs, the sandbox often exists within the cloud, which provides computational resources and for tasks like model training.
    a. Apache Spark: Apache Spark is a powerful open-source data processing engine designed for large-scale data analytics. It allows for distributed computing, meaning tasks that are broken down and processed across multiple machines simultaneously. In AI development, Spark is often used for training models on large datasets in parallel, improving scalability and efficiency.
    b. Hadoop: Apache Hadoop is another open-source framework that stores and processes large datasets across clusters of computers. Hadoop's MapReduce programming model beraks down tasks into smaller components and distributes them across many machines, making it useful for AI applications that need to handle massive amounts network data, such as those generated by ANs.
2. Runtime Mode (Production): after an AI model has been trained and validated in development mode, it moves to runtime mode, where it is deployed in the live network. In runtime, AI models operate in real-time to make decisions, optimize resources, and enable closed-loop automation.

8.2 Layered Intelligence in AN

The AN architecture applies layered intelligence across different network layers to ensure seamless coordination between business operations, service orchestration, and resource management. This multi-layered approach allows each layer of the architecture to operate semi-autonomously while contributing to the broader system's self-management goals.

- Cloud + AI Layer: the cloud acts as the central hub for AI model training and storage. It provides the necessary computational resources and data storage to train complex AI models using large datasets.
    - Cloud computing: provides an on-demand availability of computing resources over the internet, allowing organizations to store data and run applications without managing physical servers.

- Service Management Layer + AI: in this layer, AI-driven systems manage service orchestration and SLA (Service Level Agreement) enforcement, continuously adjusting services based on network conditions and demand. AI inference engines deployed at this layer process data flows and make decisions that optimize network performance.
    - AI Inference: Inference refers to the process of applying trained AI models to new data in order to make predictions or decisions. In the AN context, inference engines analyze network data in real-time, helping adjust configurations based on current network conditions.
- Network Element (NE) Layer + AI: NE are individual hardware or software components in a network, such as routers, switches, or firewalls. Embedding AI into these elements allows them to make decisions locally, reducing the need for centralized control and enabling faster responses to network changes.
    - Edge Computing: processing data at the edge of the network, closer to the data source (e.g., network elements), rather than sending it to a centralized cloud. In ANs, edge computing reduces latency by allowing AI models to make decisions at the local level, enhancing the speed and responsiveness of the network.

8.3 Developing and Using AI Models

AI models undergo a full lifecycle, from data preparation and model training to real-time inference and continous optimization. This ensures that AI systems remain effective as network conditions evolve.

1. Data Service: data service manages the lifecycle of data, from collection to processing, ensuring the quality and integrity of the data used for training. This includes data governance, which ensures data is handled in a way that meets regulatory requirements, such as data privacy and security.
2. Model Training: AI models are trained using large datasets, often throught frameworks such as TensorFlow or PyTorch. During training, feature engineering is used to extract important features from the raw data, making it easier for AI models to learn from the data.
3. Inference Framework: after training, AI models are deployed into the live network where they perform inference.
4. Standarization of AI Models: To ensure scalability and consistency across the network, AI models need to be standardized. This means ensuring that models are interoperable across different platforms and environments (e.g., cloud and and edge).

8.4 Relevant AI Technologies for AN Scenarios

Different AI technologies are applied depending on the specific needs of the network, depending on the specific needs of the network, including managing traffic, detecting anomalies, and optimizing performance.

1. Automated Machine Learning (AutoML): AutoML automates the process of selecting, training, and optimizing machine learning models. This is particularly useful in ANs, where rapid model deployment is needed to handle dynamic network conditions.
2. Transfer Learning: Transfer Learning allows AI models trained in one context to be adapted to another with minimal additional training. This is useful in Telecoms, where models trained on one type of network can be applied to another without starting from 0.
3. Federated Learning: models are trained across multiple devices without centralized data, allowing for data privacy and local optimization. This technique is particularly useful in ANs, where data privacy is a concern.
4. Knowledge Graph: represents relationships between entities, such as network elements, users, and services. AI uses this graph to infer patterns and relationships between different entities. In telecom networks, it can be used to map out connections between devices, services, and users, allowing AI to make more informed decisions.

8.5 AI in Common Telecom Use Cases

8.5.1 Perception and Prediction

Perception and prediction involves the use of AI to analyze network data and forecast future states, enabling proactive decision-making. One prominent example is energy-saving techniques in Base Transceiver Stations (BTS), where AI models predict traffic patterns and adjust operations to reduce energy consumption.

- Base Transceiver Station (BTS): critical component in wireless communication networks responsible for transmitting and receiving signals between mobile devices and the network. Reducing the energy consumption of BTS components, such as carrier amplifiers, is essential for lowering operational costs and improving sustainability.

In the case of BTS energy-saving, Long Short-Term Memory (LSTM) neural networks are commonly employed. LSTM is a type of recurrent neural network (RNN), specifically designed to handle time-series data, making it ideal for predicting traffic patterns. By analyzing historical traffic data (such as the Physical Resource Block (PRB) utilization), the LSTM model can predict future traffic loads. This prediction allows the network to configure energy-saving strategies, such as turning off or reducing the power of BTS carrier amplifiers during low-traffic periods.

- PRB: units of bandwidth used in wireless communication systems to allocate resources to users. Managing PRB traffic efficiently is crucial for optimizing network performance and reducing energy consumption in BTS systems.

8.5.2 Detection and Identification

AI is widely used in telecoms for fault detection and root cause analysis, which are critical for maintaining network reliability and reducing operational costs. The complexity of modern telecommunications networks makes it difficult to manually identify the root cause of issues such as base station power failures. AI technologies like frequent text mining, clustering, and knowledge graphs are employed to automate the identification of faults and determine their root causes.

- Frequent Item Mining: this is a data mining technique used to identify patterns that frequently occur in large datasets. In the context of telecom, frequent item mining helps identify common faults or failures that tend to co-occur in the network. For example, if a base station power failure often leads to certain transmission errors, frequent item mining can help pinpoint the most likely causes.
- Clustering: Clustering is an unsupervised learning technique used to group similar fata points together. In telecommunications, clusteringg is applied to group network elements or fault occurrences that exhibit similar behaviors. This helps in narrowing down potential causes of a network issue based on patterns of similar faults across multiple network nodes.
- Knowledge Graphs

8.5.3 Control Optimization

Refers to AI's ability to fine-tune network parameters to maximize resource utilization and enhance service delivery. In complex environments like 5G networks, manual optimization of network parameters is time-conusming and inefficient. AI systems, using RL and deep learning, can quickly explore an evaluate different antenna configurations in real time. Instead of manually adjusting settings, AI finds the optimal combination of parameters that maximize signal stregnth, minimize interference, and enhance overall quality of service.

8.5.4 Process Optimization

Process optimization in telecoms is focused on automating repetitive tasks that would typically require a human intervention, such as network maintenance and operations. Robotic Process Automation (RPA) is a key AI-driven technology in this area.

- Robotic Process Automation (RPA): involves configuring software "robots" to mimic human actions and interact with data systems in the same way a human

operator would. In telecoms, RPA is used to automate business processes, such as managing customer requests, billing, and troubleshooting network issues.

- AIOps (Artificial Intelligence for IT Operations): AIOps refers to the application of AI in IT operations, combining multiple AI capabilities (such as machine learning, natural language processing, and RPA) to enahnce the automation of complex processes in network management.

RPA tools automate tasks like customer ticket resolution, network monitoring, and maintanance scheduling. By leveraging machine learning models, RPA can predict when network components need maintenance or automatically resolve common network issues. AIOps takes this a step further by integrating AI across multiple processes, such as KPI anomaly detection, log anomaly detection, and fault detection.