AI based Adaptive Network for Smart Cities

AI Defined Infrastructure based Network

Bhagvan Kommadi
CEO: Quantica Computacao
bhagvanarch@gmail.com

***Abstract*— Self-aware, Self-Defending Adaptive Network is a network that defends itself from security breaches in the deployment of smart cities. An adaptive system that knows and recognizes the level of threat faced by an intrusion across a network of smart cities. To detect and separate security threats, the AI program uses a new method of machine learning to track any aspect of a network. Threats include ransomware, high-jacking code, intrusion and illegal entry, theft, and unauthorized use. An autonomous system comprises of a collection of autonomous modules that are introduced and removed dynamically. To order to achieve machine objectives, nodes inside such an ensemble will cooperate. In response to changes in its operating environment, the self-adaptive network modifies its own behavior. We mean anything that the network can observe, such as user interaction, network devices and sensors, or instrumentation, by operating environment.**

Keywords—adaptive network, AI defined infrastructure, smart cities

I. INTRODUCTION

Adaptive network with AI is used for automated service provisioning. The network providers automate manual service lifecycle processes. These process are automated using in packet and optical networks. Packet and Optical networks are built using a software defined networking based automation platform. The automation platform is multi-layer and multi-vendor based which adopts DevOps processes. For instance, a network provider can automate the delivery of its wavelength services and plans. They can automate to extend this platform to other services using a phased approach.

Proactive network assurance is another area where AI based adaptive network can be used. The network providers want to identify and correct as many network issue that they can foresee and predict. This helps in increasing network reliability and deliver with specified SLAs. AI based adaptive platform improves the customer experience. This platform will have features related to pre-emptive network maintenance across the optical, Ethernet and IP Wide Area Networks. AI based automation platform will have the network health prediction capabilities. Along the same lines, Machine learning based analytics can predict the likelihood of a network node's failure in a given timeframe for repair.

AI based Adaptive network can help in Fiber capacity analysis and optimization. Policy based matching of channel and wavelength capacity improve the efficiency and adaptive planning of optical networks. Providers can predict signal variability by combining real-time network telemetry data and traffic forecasting with AI based predictive analytics. This helps in improving the system margin utilization and reduce cost-per-bit.

II. AI-DEFINED INFRASTRUCTURE

AI Defined infrastructure can manage planning, build, run and maintain tasks. In Planning tasks, AIDI is used for analyzing the demand trends and predicting the infra requirements. Using the requirements, planning can be done appropriately. We can also ensure the infrastructure is according to the requirements.

In build task, the necessary resources can be deployed as per the workload requirements. Resources can be deallocated when there is no need. The infrastructure components can be configured easily. In the run and maintain tasks, AIDI can be used to analyze the data patterns. The data patterns help in indicating the behavior of the system. The behavior of the system helps in making the model of the system behavior. AI based training helping in building this model with quality parameters. The quality parameters which are used for the model are availability, scalability and storage.

The anomalies in the network can be identified by the AIDI based platform. Intrusion detection, fraud points, fault points, infrastructure abuse and failure are the anomalies identified. The platform can detect the threat and act to rectify and fix the problem. It has features to react or proactively act based on the single or group of infrastructure components. Errors can be fixed completely by autonomous actions. AIDI helps in reducing the cost of IT infrastructure. The cost is reduced by using the most optimal components.

III. CHALLENGES IN EXISTING NETWORKS

Network providers are now rethinking about their operations with Artificial Intelligence. AI can be used to achieve the long desired goal of end-to-end automation. Automation might remove humans from the equation. The network providers want their networks and operations to become adaptive. This is to respond to a changing competitive landscape and consumer demands. These demands require a coherent combination of human-controlled and supervised automated operational processes. They might also need analytics-driven intelligence, and a programmable infrastructure.

The evolution to 5G and IOT adoption is putting massive pressure on today's networks. There is need to increase the capacity by orders of magnitude. On the related front, the networks need to have the ability to respond to unpredictability in traffic patterns.The optical network which is at the heart of communications helps in interconnecting people, data centers, and devices in the network. The network need to meet today's web-scale demands.

Operators are having challenges in handling bandwidth demands. They are managing the demands by deploying,

managing, and sparing different hardware. They are using cost-optimized solutions per specific application. They select the hardware based on the best-guess fiber characterization data. Lack of network visibility and efficiency is forcing operators to operate at suboptimal capacity. These factors are making the operators lose revenue resulting in costly network overbuilds.

Fig. 1. Current Day Networks

IV. ADAPTIVE NETWORKS

Adaptive Network platform based on AI will have three important components which are software control, programmable infrastructure and analytics driven intelligence. The software control forms the basis of adaptive operations. The basis is supported by the automated creation and deployment of network services. These network services are deployed for scale and speed using software defined network, Network functions virtualization and open APIs.

The programmable infrastructure is a hybrid future generation network. It comprises of open, software defined network enabled physical networks and cloud-native virtual network functions. It will provide advanced telemetry that delivers real-time data on the health of the network. The programmable infrastructure will provide the ability to match the changing capacity needs.

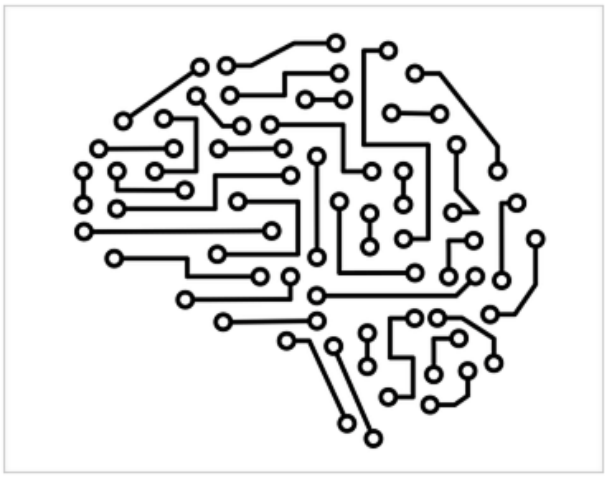

Fig. 2. Adaptive Network

Another component named Analytics-driven intelligence enables intelligent automation. The intelligent automation enhances autonomous decision making and supporting software-control. They can achieved through policy management, rule engines, AI, machine learning and telemetry. We need to have a robust storage repository. The repository will record, process and aggregate real-time and historical large-scale and raw data streams. The data streams such as log files and telemetry data are recorded in the repository. The raw data will be processed, normalized and used for advanced data models and analytics algorithms. These algorithms are used to generate actionable insights.

Network providers will apply different kinds of machine-learning techniques. These techniques are based on the operational use cases and benefits. The techniques used are supervised learning, reinforced learning and unsupervised learning. Supervised machine-learning based algorithms are trained to identify patterns such as degrading network performance. They can also be used to predict an outcome like port failure and trigger remediation actions such as auto-adjust network bandwidth and add new capacity. This technique is commonly used and suitable for use cases in which historical data and outcomes are known. Reinforced learning involves continuous calibration of these algorithms based on previous feedback on actions. Unsupervised learning algorithms use grouping and clustering techniques to organize data. This helps to understand the structures and enable the discovery of patterns. The patterns discovered are related to previously unknown and unnoticed scenarios such as identify new user, service traffic behavior and profiles. These patterns are used to improve forecasting in network planning.

V. SELF-AWARE, SELF-DEFENDING ADAPTIVE NETWORK

Self-conscious, Self-Defending Adaptive Network system is a smart agent-based system that tracks network activity, information, and actions. Data focused on network activity, material and action is used to recognize and combat various forms of cyber threats.

The architecture of the intelligent agent knows and recognizes the level of threat faced by a node in a network. To order to identify and separate cyber security risks, the adaptive network architecture employs machine learning methods to track the network. The known security threats include ransomware, high-jacking code, intrusion and illegal entry, piracy and unauthorized usage. This requires the self-awareness, self-protection and adaptation of all properties to any external or internal danger. This approach eliminates the possibility of zero-day attacks. This is because anomalous packet actions and information can be observed by the network. The adaptive network self-learning device learns through use and becomes wise with time.

Fig. 3. Secure Network

The self-conscious, self-defending adaptive network system will understand the actions and quality of each packet. The actions and content are used to assess whether the trend is predicted or anomalous. It helps you determine whether it is a danger to search and find out. This adaptive and associative network senses increasing byte in the system's partnership. It is able to identify trends in known threats. It can detect anomalous trends and distinguish them. The identified anomalous patterns may be associated with a zero-day attack, non-compliant network use, or sabotage.

To demonstrate an efficient self-learning network, we are looking at the neocortex's individual neural network. A clever system, influenced scientifically, acts as a human brain. The human brain will learn autonomously at the moment of stimulus by recognizing patterns. The adaptive network, like human brain, stores each special byte sequence. The values such as stimulus date, location of stimulation, pattern format, packet payload and addressing are retained each time the pattern is observed. The data model stored has a n-dimensional representation of each pattern's semiotic value..

VI. INTENT BASED NETWORKS

Intent-based networks are used to identify the business-related meaning. It will bridge the gap between enterprise and IT. The advantages of purpose-based networking are linked to the potential to intelligently simplify network management and orchestration. These reflect a solution set that is the confluence of key technologies such as machine learning, Artificial Intelligence, Software Defined Networking and Internet of Things technologies.

VII. CONCLUSION

The new network infrastructure system is Cognitive Network Management. Network operators used proven Self-Organizing Network systems to implement and run networks. Mixed with Software Defined Networking and advanced analytics, artificial intelligence brings the automated, cognitive activity and management of the network to the next level. The combination of machine learning, software-defined network, and data analytics innovations will quickly lead to early and comprehensive performance in cellular networks. Due to self-awareness, self-configuration, self-optimization, self-healing, and self-protection, the future economic and social gains can be accomplished.

By developing 5G networks, we must understand such opportunities. Through technology such as Machine Learning, Software Defined Networking, Network Function Virtualization, Network Slicing, Quality of Service Management, and new security methodologies, network architectures can be implemented.

REFERENCES

[1] ANFIS: adaptive-network-based fuzzy inference system J.-S.R. Jang

[2] A neural network based feedforward adaptive controller for robots R. Carelli ; E.F. Camacho ; D. Patino

[3] Adaptive delay-based congestion control for high bandwidth-delay product networks Hyungsoo Jung ; Shin-gyu Kim ; Heon Y. Yeom ; Sooyong Kang ; Lavy Libman