https://doi.org/10.5755/j02.eie.38680

Paramounts of Intent-based Networking: Overview

Martins Mihaeljans*, Andris Skrastins, Jurgis Porins
Institute of Photonics, Electronics and Telecommunications, Riga Technical University,
10 Zunda Embankment, LV-1048, Riga, Latvia
**martins.mihaeljans@edu.rtu.lv; andris.skrastins@rtu.lv; jurgis.porins@rtu.lv*

***Abstract*—This study is an exploration of the design of the state-of-the-art intent-based networking (IBN) model. In IBN, communication means are initialised by user's (herein IT staff, not end-user) input of requirements and not instructions. Thus, allowing the self-organisational abilities of the network to set communication paths. Through research of academic studies and standardisation drafts we conduct IBN structure. We determined the need for change in the design. The current IBN model detains its adaptation as network assurance requirements of ensuring network security and scalability, and continuity are unfulfillable via conduct of network analysis and track of intent drift. We propose two submodels - one for autonomous networks and one for supervised networks.**

***Index Terms*—Intent-based networking; Internet of things; Network function virtualisation; Software defined networking; Service function chaining.**

I. INTRODUCTION

"None of us just live in a silo. Everything is in context", U.S. VP K. Harris states and emphasises that "You exist in the context of all in which you live and what came before you" [1]. This is pertinent to intent-based networking (IBN), where the subject must integrate and preserve the surrounding structure. In essence, artificial intelligence (AI) augments the network control and management processes previously overseen only by man.

IBN users do not necessary have knowledge of the structure of the network, but they can express desired intentions as requests. The interpreter transforms the request into a configuration. An actuator then enables the newly generated configuration. Finally, assurance ensures intents fulfilment. IBN is highly dependent on AI and machine learning (ML) capabilities, from intent profiling through natural language processing (NLP) to predicting network accessibility through big data and generative adverbial networks (GAN) [2]–[6].

In this paper, we investigate the basic building blocks of IBN and its working principles. The outcome of this research is a proposal for a division of autonomous and supervised IBN. Network assurance is a stumbling stone for IBN adaptation [6]. The basis is sorted in Table I. The selection criteria were accuracy, relevance, and scope of information.

TABLE I. SCOPE OF THE OVERVIEW.

Material type	Count	Reference index
Academic studies	20	[8]–[11], [13], [15]–[18], [20]–[30]
Recommendations	4	[2], [3], [4], [12]
Surveys	5	[5], [6], [7], [14], [19]

Manuscript received 19 May, 2024; accepted 28 September, 2024.

II. STRUCTURE OF INTENT-BASED NETWORKING

IBN has five building blocks (Profiling, Translation, Resolution, Activation, and Assurance). The blocks form two closed loops (combination of all five and combination assurance-resolution-activation) shown in Fig. 1.

IBN is supposedly set to achieve a trinity of assessment - self-organisation, self-reconfiguration, and self-optimisation. One loop facilitates the entire lifespan of intent, while the other provides assurance (a perpetual enhancement process of intent assessment via analysis of network state) [5].

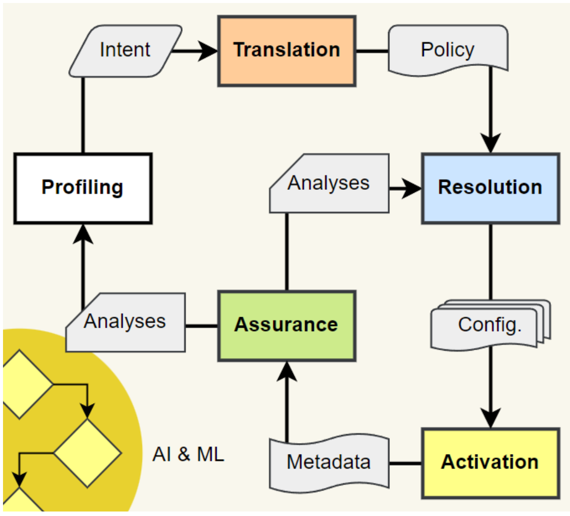

Fig. 1. Intent-based networking model.

The survey in [5] has also meticulously examined the applicable underlay technologies and extracted a set of IBN open issues in conjunction with possible solutions, which are:

1. The alignment of intents expression with translation could be resolved by classifying user's experience;
2. Business-specific intents can be fulfilled if IBN is auto-adaptable and auto-configurable;
3. Improve the vocabulary of neural language processing by using of chatbots and incremental learning for IBN to adopt the user's language and not vice versa;
4. Network assurance and available datasets could be leveraged from the combination of ML profiling and transfer learning method;
5. Zero-touch aka autonomous networks can only be achieved via use of AI in control theory application;
6. Multi-domain network management is obtained by structuralising network controllers in a hierarchy.

This problem-solution list is nonexhaustive and at hand states the general areas of interest for IBN model deployment.

A. Profiling of User Request/Desire

Often an intent is not something that is directly feasible from the amount of information presented to the interpreting system [7]. Users of IBN can be with, with some, or even without any knowledge of actual network structure and capabilities. Thus, intent proposal does require undergoing an assessment and correction mechanisms. Those might be incorporated into profiling techniques shown in Fig. 2.

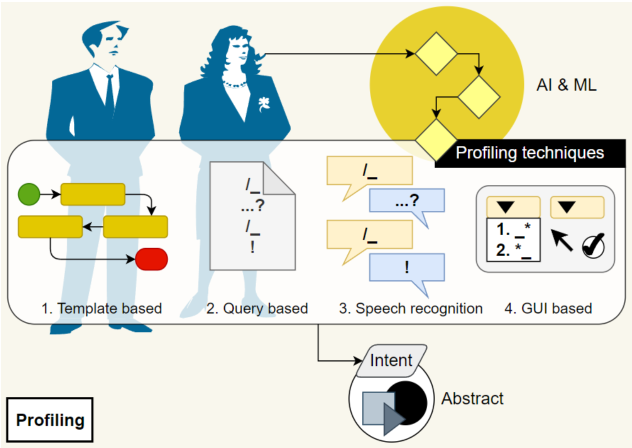

Fig. 2. Intent profiling building block.

1. Template-based - The user is taken through set of predefined attributes and preferences to set up an intent.
2. Query-based - The intent is discovered via the initial input and an acknowledgement cycle where additional information is requested via secondary input from the user.
3. Speech recognition – A keyword extraction from speech or text-based input with the help of NLP [8].
4. GUI-based - User is presented with dashboard of network pseudoconfiguration settings.

The profiling techniques in use do not depend as much on the preferences of users as on their ability to understand technicalities. Examples of users and their intents are:

– Beginner (helpdesk operator) - Alert on connection issues at branch offices;
– Competent (service technician) - Optimise link utilisation for high-quality voice communication needs in headquarters for weekdays nine-to-five;
– Advanced (project manager) - Enforce government regulation compliance on all logged data for past quarter;
– Proficient (software developer) - Secure transactions and system calls made to and from test environments;
– Expert (network administrator) - Prioritise business critical application workflow continuity for minimal network traffic flow migration during peak hours.

As shown in the examples above, intent itself is an abstraction and not a set of performable actions. In addition, more experienced users might be granted with privileges of supervision, and abilities to overthrow other user intents.

B. Translating Intent into Underly Appropriate Policy

Application of an intent cannot begin without fitting the task to subattribute of event, action, condition (EAC). EAC is a basic declaration of a rule in policy-based management systems. Such systems have been in action to manage network traffic in network functions such as firewalls for more than a decade [2].

For translation, different mechanisms can be utilised, such as blueprint, mapping, refining, graph-based, ML, etc. Whichever mechanism is in use, the outcome must form an appliable network configuration with no abstraction. A standardisation draft [4] defines an IBN language specifically for intent modelling. A study in [9] extends it with the ability to define policy definitions reactively.

While intent is a high-level abstract descriptor, a policy is a low-level descriptor due to its nature of need for structure and configuration. Intent translation is shown in Fig. 3.

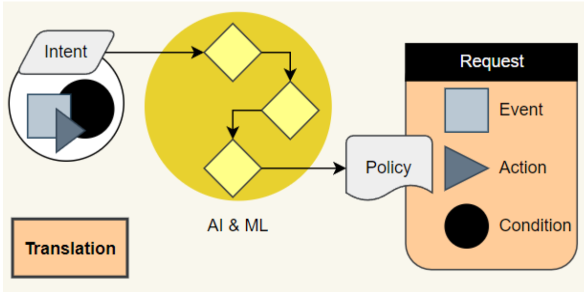

Fig. 3. Intent translation building block.

C. Resolution of Intents Footprint

When intent is descriptive enough to be accommodated into the underlying system, a mechanism of try/catch must be run for disclosure of the effect its application might generate. Touched systems must persist serving all previously enacted intents if an overwrite is not the intended purpose of change.

A prediction of possible intent drift is possible with a combination of the intent database and previous network state snapshots. These predictions could be ML generated or could also be clause-based logical decisions. Network slice load prediction and resource forecast, as well as load balancing and anomaly detection, or user mobility prediction, are just some examples of IBN tasks performed by AI and ML [10].

In case of resolution failure, IBN can notify the user and restart the profiling process. Although IBN is intended to be an autonomous, close to a one-touch environment, that does not mean it incorporates one-shot policy. Users are required to input their intents once, and the rest of intents lifecycle is facilitated by IBN. However, users are required to oversee intents creation process as corrective actions may be needed. Intent resolution is shown in Fig. 4.

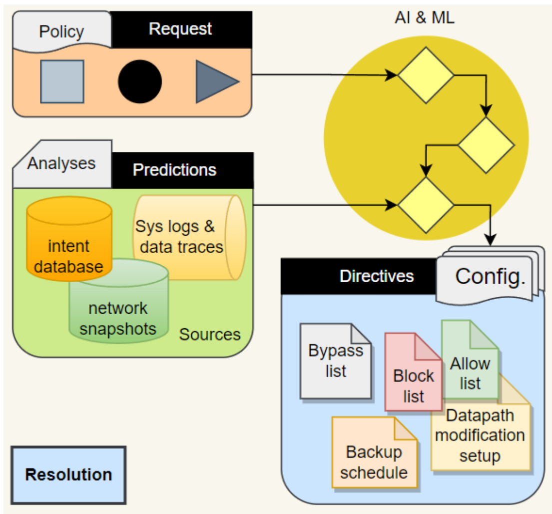

Fig. 4. Intent resolution building block.

D. Actuating the Necessary Modifications

In a state of compliance with the existing system, intent can be deployed. This IBN building block is where the actual underly network gets affected. Changes to existing network fabric can include but are not limited to network traffic flow migration, quality of service (QoS) assessment, datapath modification, or even server migration to other premises.

Service function chaining (SFC) and network function virtualisation (NFV) are the main underlying technologies leveraged for intent deployment. However, no changes are error-prone, therefore, when making any modifications a snapshot of the network configuration, as well as the rest of the intent states, is required to be taken. This can serve for both immediate rollback and as a reference point for intent drift remedy upon subsequent discoveries. Intent actuation building block is shown in Fig. 5 where the configuration from the resolution block is inserted into the network fabric and metadata of the network state is collected afterwards.

It is important to note that network fabric can rely on both IBN orchestration and local orchestration from within placed network controllers.

An essential component of IBN is the single source of truth. This component handles the informational structure of the intent and ensures that all related parties (user, network controllers, and network fabric) have the same understanding of the intent and its current state and application goals.

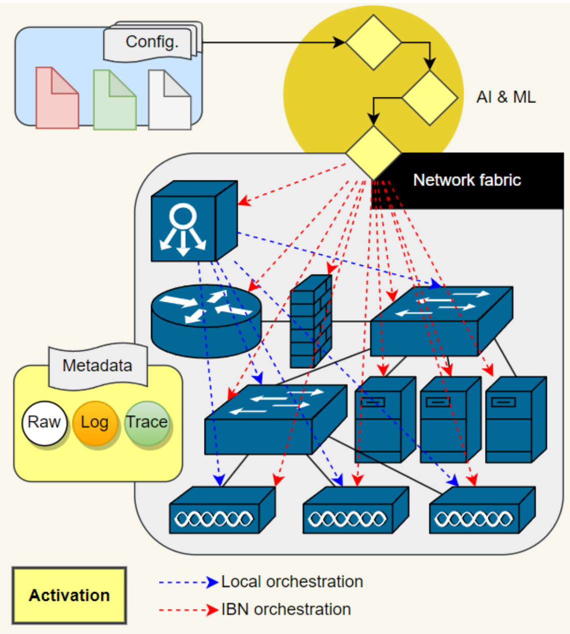

Fig. 5. Intent activation building block.

E. Assurance of Operational Successfulness

Continuous monitoring of the system enables detection of intent state and whether the original user request is fulfilled. Intent fulfilment is not a stationary state, therefore, upon successful deployment assurance keeps track of necessary optimisations and adjustments.

Assurance is the key element in IBN, which enables the functionality of the rest of the building blocks. Its primary objective is to monitor the passive and active systems. The types of monitoring can vary between different parts of the network fabric used for the deployment of each intent. The followings are some examples:

– On access network - End user mobility and density, interference, and signal-to-noise ratio (SNR);
– In data centres (DCs) - CPU, RAM, and storage utilisation, virtual machine (VM) states;
– For optical networks - Quality of transmission, optical power, optical SNR;
– Generic values - Round trip time, jitter, packet delivery/error ratio, or queue size [6].

The intent assurance building block shown in Fig. 6 also ensures a single version of truth, which is a component used for database querying, information pulling, and data filtering for correlations related to single intent within multiple parts of the network fabric.

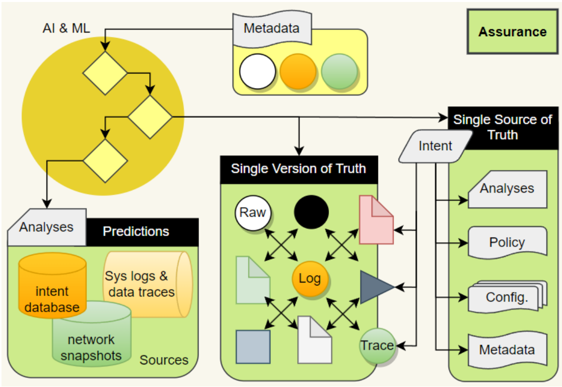

Fig. 6. Intent assurance building block.

Another important aspect to maintain abstraction at a building block of profile is security as providing users with network transparency raises potential risks of atrocities [11].

III. UNDERLAY TECHNOLOGIES

IBN does not target to redefine existing networking principles of switching, routing, and forwarding, or any other packet processing mechanism. It also does not intend to reinvent operations, administration, and management (OAM) application techniques. Its primordial objective is to take control over all these functions whilst leaving capability of higher-level supervision to its users. Therefore, an underlay technology used for intent structurization can be, but is not limited to, policy-based network management (PBNM). Even more so, IBN potentially would utilise the same existing mechanisms as policy decision point (PDP) and policy extraction point (PEP) for intent instantiation.

A. Artificial Intelligence

As reported in [12], artificial intelligence (AI) does have a set of problems that need to be overcome for its application in network management. A nonexhaustive list is as follows:

1. Huge solution space - Try-catch of every possible aid is impractical;
2. Unpredictability - A continuous change in network state makes forecasts unreliable;
3. Demand window - Solutions must arrive in a timely manner to be used for problem management;
4. Dataset dependence - Solutions are as accurate as are ML training sets and if they hold applicable cases;
5. Integration with existing management systems;
6. Cost-efficiency - When distributed AI is used on edge or in the forwarding plane, processing resources are limited.

As a subset of AI, machine learning (ML) and big data are a cornerstone of intent-based networking development. Together these technologies are utilised in all five building blocks of the model accordingly:

– Profiling - Natural language processing (NLP) allows for human speech recognition making the interpreter function much like voice assistant;

– Translation - Template-based fitting translation, as well as keyword and phrase structure extraction, for policy generation;

– Resolution - Comparison of multiple monitoring datasets in conjunction with the intent of the user and network configuration database check;

– Actuating - Resource management and allocation trade-off operation automatization and more complicated task handling as network traffic flow migration planning and execution;

– Assurance - Continuous monitoring optimisation according to network availability fluctuation and autonomous state snapshot generation for future intent lifespan analysis, including but not limited to intent drift extraction.

The authors of [13] used long short-term memory (LSTM) ML models and convolutional neural network (CNN) to predict CPU usage in virtual machines (VM) for a short future timeframe. It is also proposed that assurance engine design may vary for different use-case scenarios.

Some areas are less mature than others. For example, learning of network states and predicting possible hiccups is limited by the quantity of qualitative datasets gathered from network troubleshooting. In aid, a generative adverbial network (GAN) can help generate missing cases [6].

B. *Software-Defined Networking*

Unlike legacy network devices in which communication configuration capabilities are directly imprinted and burnt into local memory (switches, routers, firewalls, etc.), software defined networking (SDN) devices facilitate centralised management and configuration approach. SDN is one of the crucial technologies under the IBN concept as it is organised into three easily distinguishable planes as follows:

– Application plane - Accommodates user (usually network administrator or similar) interaction with the network through policy-based network management (PBNM), which is imposed on underlay control plane via application programming interface (API) or RESTful functions;

– Control plane - Receives users' declaratives and transcribes them into network configuration which is broadcasted to all implicit forwarding devices that reside in underlay forwarding plane;

– Forwarding/data plane - Executes network traffic forwarding according to configuration imposed by control plane. Unlike L2 switching or L3 routing, forwarding is a packet processing mechanism that can extract any packet header information to match network traffic with specific flow entry for distinguishing the right packet transmission path.

The SDN design model is shown in Fig. 7 where the operations, administration and management (OAM) channel directs network policy implementation while the data channel showcases end device communication. Featured in our recent research on Internet of Things (IoT) and SDN fusion [14], this SDN model represents the very own logic of indirect device configuration as the user (resides in the application plane) only directly accesses the network controllers. The study in [15] notes that SDN by itself lacks the closed-loop data analytics (assurance-resolution-activation) that is needed for autonomous networks and is a part of IBN. Research in [15] states that partial implementation of IBN is due to the challenges facing a comprehensive framework, how to align intent with user requirements, how to translate intent into network configuration, and how to ensure intent fulfilment.

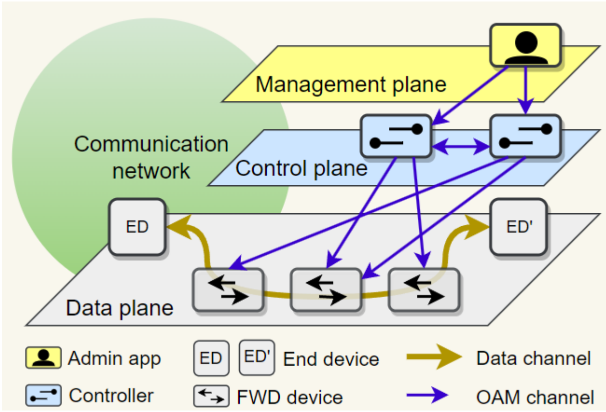

Fig. 7. SDN design model [14].

It is common to link SDN with only data centre (DC) networks as most of the backhaul technologies relies on legacy network capabilities (L2 switching at network access and L3 Border Gateway Protocol at core backbone).

Due to rapid industrialisation, the enterprise has spawned its industries into multi-domain tenants. For example, multiple companies can share same data centre, rack, or even server but at the same time have a secondary placement in their headquarters and/or branch offices. The graphical user interface (GUI)-based multi-domain IBN model for virtual network function (NF) scaling for the evolved packet core (EPC) has been introduced in [16].

Software defined wide area network (SD-WAN) solutions such as Cisco Meraki (centralised network access device management) or Quagga routing suite (SDN edge software for legacy network protocol control from Linux OS) allow one to limit the gap between multitenant needs and core network capabilities. For example, in [17] the authors studied how the number of SD-WAN branches affects the intent deployment time.

Although for many years OpenFlow protocol and its eligible hardware/software like open virtual switches (OVS) were an industry standard for an SDN implementation, nowadays it is being replaced by a more robust approach, Programming Protocol-Independent Packet Processors (P4).

The limitation of OpenFlow lies in its inability to redefine the function set of the device (match, set IP source field, push VLAN, pop VLAN, etc.) from the get-go. Users still needed to wait for the manufacturers to implement the necessary functionality through an update or upgrade. However, P4 allows one not only to manipulate with existing functionality, but to also rebuild it or add a new one to white switches (networking devices with possibility of reconfiguration) [18].

A plethora of scientific research regarding SDN has been done via the use of the Ryu controller and Mininet network emulator. The authors in [19] created an IBN framework for AI-based intent perception and fulfilment. By conducting a survey, the authors in [19] discovered that AI is commonly used for input or management of the intent, but not fully throughout the IBN structure.

C. *Network Function Virtualisation*

DC networks can become oversaturated with inbound and outbound network traffic not only at a peek hour, but also due to unexpected application behaviour or improper data backup generation schedules.

Some data traffic is supposed to leave DC premises, but other only needs to travel as far as neighbouring server appliance or even adjacent blade of same server.

There are instances where various applications reside in same server (Kubernetes, Docker, OpenShift, etc.) but require distinct barrier between for security reasons.

In all mentioned cases, a virtualised network traffic processing device can come in aid as a trade-off between the need for packet switching speed or placement and functionality among closely resided resources.

Any network function (NF) can be virtualised - routing, switching, forwarding, network address translation (NAT), deep packet inspection (DPI), etc. In research in [20], virtualised NF placement is studied for an abstract user intent satisfaction in a multitenant environment.

D. *Service Function Chaining*

Due to the development of network function virtualisation (NFV), a paradigm of steering network traffic through a customised NF path has emerged in the form of service function chaining (SFC). We have extensively covered SFC in study [21], but in summary, the SFC domain shown in Fig. 8. consists of the following elements:

– SFC network traffic encapsulation-aware network functions (NFs), aka service functions (SFs), SF classifiers, and SF forwarders;

– A SF chain is the designated array of SFs that network traffic should traverse for service delivery, but an SF path is the actual datapath taken;

– SF forwarders are nodes that do not modify network traffic in any way but only pass the network traffic from one SF to another. SF classifiers impose and remove SFC encapsulation on to network traffic packets;

– Utilisation of additional encapsulation allows one to alter network traffic path from one that would be taken by L2 switching or L3 routing.

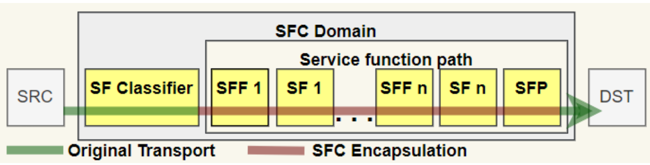

Fig. 8. Service function chaining domain [21].

We also covered service function chaining in [22] from the perspective of automation for network traffic classification at SFC domain ingress. We proposed reactive path discovery at the time of traffic arrival instead of proactively defining all possible paths. The main drawback of our method was the time needed to select an appropriate service function selection. AI could potentially mitigate it by generation of sophisticated selection patterns.

In our recent study in [23], we used SFC encapsulation abilities to differentiate between multipath transmission control protocol (MPTCP) subflows belonging to the same session for bandwidth utilisation optimisation. Similarly, the study in [24] approaches the necessity for fair resource allocation and deals with the detection of conflicts among intents generated by multiple users. The study in [24] claims that IBN use in SDN rises a security issue where abstraction of centralised control enables possibility of illegal access.

IV. Implementation Domains

As a multipurpose system, IBN can be deployed in a variety of domains and serve not only for communication means, but also for businesses, healthcare, social security, etc. Below are some of the domains of interest.

A. *Enterprise Networks*

– Operational technology - Management of intents related to manufacturing, monitoring, and control systems in industrial environment.

– Information technology - Management of intents related to LAN, DCs, and Cloud resided end device end-to-end communication enablement.

Research in [25] delves into the quality of service delivery capabilities of IBN as it eludes on the transition away from traditional networking in enterprise environments.

B. *Operator Networks*

5G communication autonomy evolvement for ML is used in radio access networks (RAN). Here, the importance of a proper antenna tilt is just as high as one for adequate network slicing. The authors in [26] developed an IBN compliant monitoring framework capable of monitoring active and passive RANs by using network function virtualisation (NFV). Tools utilised for data collection and querying were Prometheus, Elasticsearch, and Grafana.

C. *Internet of Things*

The widespread adaptation of Internet of Things (IoT) technologies in monitoring and control systems, such as sensor and actuator networks, has created a need for SD-WAN solutions for automation and maintenance of these autonomous devices.

Recently, the IoT has achieved another milestone by overcoming the lack of interoperability in consumer products. Matter protocol and Thread communication technology have made smart home IoT devices attractive to new buyers, as they no longer must worry whether one device will work with another. We studied these technologies in [14] where we discovered that the inadequate ambiguity of IoT standards halts the conceptional model from ever gaining a common framework for IoT device design.

Research in [12] states that the lack of a human-understandable reasoning process is an aspect that makes AI and ML solutions unattractable for implementers in networking domains. Often guarantees in the form of service level agreements (SLA) must be met. Therefore, black-box behaviour has no place in ensuring SLA compliance.

V. PROPOSED IBN SUBMODELS

Assurance is responsible for intent fulfilment by ensuring the security and scalability and continuity of the network via conduct of network analysis and track of intent drift. The open challenges for assurance are as follows:

1. Bilateral user intent intervention - Ensuring that one user's intent does not negatively affect other users' intent;
2. Resource allocation - How to ensure a fair use and proper distribution of network slices during normal usage, peak load, and disaster recovery scenarios;
3. Intent supervision - Ensuring intent fulfilment and escape already existing intent drift.

Hence, we propose splitting the IBN model into two. One of them could be automation-orientated and remove multiple user and new intent requirements. The other could be suggestion-orientated leaving the network configuration in the user's hands and having assurance for analysis gathering, therefore, removing resource allocation requirement.

A. *IBN for Autonomous Networks*

IoT network-like connections does not necessarily require human intervention. For example, Thread technology has self-organisation and self-reconfiguration capabilities, but on topology changes, Thread networks tend to suffer link breakages due to the personal area network regeneration process. The issue had been encountered in our previous research [27]. Respectively, intent-based networking (IBN) could assist in stray node pickup.

Other domains such as ad hoc or vehicular networks could benefit from IBN capabilities of cloud and edge computing orchestration. Figure 9 shows the IBN for autonomous networks. We suspect that many IoT solutions targeting smart home equipment will be Matter enabled. Matter is aimed towards ease of product development cycle with its core function of cross-platform application layer. This layer might include intent resolution building block functionality where lower layers could reside in subsequent blocks leaving only the initial profiling up to developer.

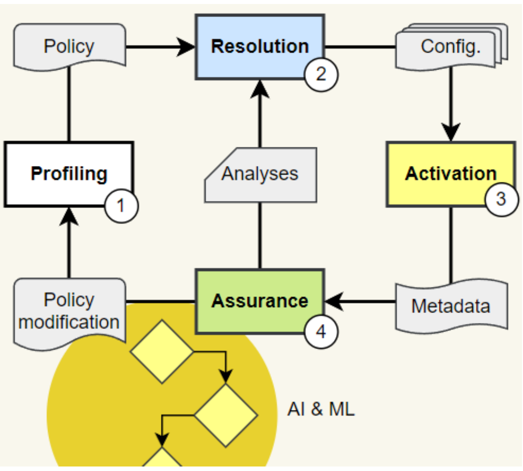

Fig. 9. IBN for autonomous networks.

From the profiling building block, an initial policy (generated by the manufacturer or user) enters the resolution block from where the second IBN loop is ignited. Once assurance detects a modification necessity, it generates a policy modification request. Intents would still be an essential part of this model, but they would reside only in the assurance building block for intent drift discovery.

B. *IBN for Supervised Networks*

Operator networks most often span across at least one autonomous system (AS), whether it is an Internet service provider (ISP) or a mobile service provider. AS are supposed to interact with each other, requiring supervision as a strict part of management. IBN enables a loosely coupled inter-working between applications in autonomous systems whilst leaving technical supervision to operators [28].

A domain accommodating networks of a not so colossal scale but of a high importance is healthcare. Telemedicine and operational medical equipment, as well as life support systems, could make use of IBN capabilities [29].

Figure 10 shows IBN for supervised networks. In this model, users set up network policy and from assurance receive intent suggestions for network optimisation. However, an ability to ingest an intent also stays possible as a secondary option for a nonexpert level user.

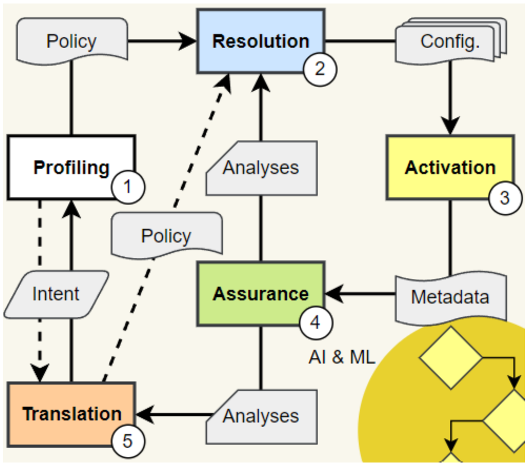

Fig. 10. IBN for supervised networks.

VI. CONCLUSIONS

In this paper, we study the intent-based network (IBN). In IBN, the governance, optimisation, and maintenance of the communication network are achieved with the assistance of artificial intelligence (AI) and machine learning (ML). The intent is a user's expressed request of the necessary outcome without formulating how the result should be achieved.

We outlined IBN structure based on the two-loop intent lifecycle (Fig. 1), making this paper the first refinement of the IBN graphical illustration since early Cisco Press materials.

We conduct that IBN has a significant reliance on AI and ML to the extent that full-featured IBN implementation is unfeasible due to insufficiency of network knowledge base.

The complexity of end-user services makes it hard to predict and detect the effect of intents ingestion. This problem can be mitigated through use of sophisticated systems such as the digital twin of a physical network [30].

A partial implementation of IBN is common among the studied materials. Studies suggest that AI is used for input of intent or network management, but not both. The design of the IBN architecture is based on the network requirements, expected outcomes, and user priorities [3].

We propose to separate implementation of the IBN for autonomous networks (Fig. 9) and supervised networks (Fig. 10) until maturity of AI and ML is raised to adequacy in complex task execution. It could relax assurance building block challenges such as intent drift tracing, intent conflict prediction, network state, and resource utilisation forecasting.

Our proposal also touches on bridging the gap between feature-enrichment equality between both types of networks, where nowadays it is supervised networks that have a Swiss-knife of toolset in comparison to autonomous networks.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] K. Harris, "Remarks at White House event", Vice President of the United States, May 10, 2023, pp. 48–49. [Online]. Available: https://sites.ed.gov/hispanic-initiative/files/2023/09/2023.5.10-FINAL-Commission-Transcript.pdf

[2] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, "Intent-based networking - Concepts and definitions", RFC 9315, 2022. DOI: 10.17487/RFC9315.

[3] C. Li, Y. Cheng, J. Strassner, O. Havel, and W. Xu, "Intent classification: draft-li-nmrg-intent-classification-01", IETF Network Working Group, 2019.

[4] S. Hares, "Intent-based Nemo overview draft-hares-ibnemo-overview-01", IETF Internet-Draft, 2016.

[5] A. Leivadeas and M. Falkner, "A survey on intent-based networking", *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 625–655, firstquarter 2023. DOI: 10.1109/COMST.2022.3215919.

[6] A. Leivadeas and M. Falkner, "Autonomous network assurance in intent based networking: Vision and challenges", in *Proc. of 2023 32nd International Conference on Computer Communications and Networks (ICCCN)*, 2023, pp. 1–10. DOI: 10.1109/ICCCN58024.2023.10230112.

[7] B. E. Ujcich, A. Bates, and W. H. Sanders, "Provenance for intent-based networking", in *Proc of 2020 6th IEEE Conference on Network Softwarization (NetSoft)*, 2020, pp. 195–199. DOI: 10.1109/NetSoft48620.2020.9165519.

[8] Y. Xiao, W. Quan, H. Zhou, M. Liu, and K. Liu, "Lightweight natural language driven intent translation mechanism for intent based networking", in *Proc. of 2022 7th International Conference on Computer and Communication Systems (ICCCS)*, 2022, pp. 46–51. DOI: 10.1109/ICCCS55155.2022.9845995.

[9] Y. Tsuzaki and Y. Okabe, "Reactive configuration updating for intent-based networking", in *Proc. of 2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 97–102. DOI: 10.1109/ICOIN.2017.7899484.

[10] K. Abbas, T. A. Khan, M. Afaq, and W.-C. Song, "Ensemble learning-based network data analytics for network slice orchestration and management: An intent-based networking mechanism", in *Proc. of NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 2022, pp. 1–5. DOI: 10.1109/NOMS54207.2022.9789706.

[11] A.-R. Meijer, L. Boldrini, R. Koning, and P. Grosso, "User-driven path control through intent-based networking", in *Proc. of 2022 IEEE/ACM International Workshop on Innovating the Network for Data-Intensive Science (INDIS)*, 2022, pp. 9–19. DOI: 10.1109/INDIS56561.2022.00007.

[12] J. François, A. Clemm, D. Papadimitriou, S. Fernandes, and S. Schneider, "Research challenges in coupling artificial intelligence and network management", Internet Research Task Force (IRTF), Internet-draft-irtf-nmrg-ai-challenges-03, Mar. 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-irtf-nmrg-ai-challenges-03

[13] X. Zheng and A. Leivadeas, "Network assurance in intent-based networking data centers with machine learning techniques", in *Proc. of 2021 17th International Conference on Network and Service Management (CNSM)*, 2021, pp. 14–20. DOI: 10.23919/CNSM52442.2021.9615580.

[14] M. Mihaeljans and A. Skrastins, "IoT concept and SDN fusion in consumer products: Overview", in *Proc. of 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2023, pp. 1–6. DOI: 10.1109/ICECCME57830.2023.10252518.

[15] H. Yu, H. Rahimi, C. Janz, D. Wang, C. Yang, and Y. Zhao, "A comprehensive framework for intent-based networking, standards-based and open-source", in *Proc. of NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, pp. 1–6. DOI: 10.1109/NOMS56928.2023.10154454.

[16] T. Ahmed Khan, K. Abbas, J. J. Diaz Rivera, A. Muhammad, and W.-c. Song, "Applying RouteNet and LSTM to achieve network automation: An intent-based networking approach", in *Proc. of 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2021, pp. 254–257. DOI: 10.23919/APNOMS52696.2021.9562499.

[17] R. Perez, A. Zabala, and A. Banchs, "Alviu: An intent-based SD-WAN orchestrator of network slices for enterprise networks", in *Proc. of 2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021, pp. 211–215. DOI: 10.1109/NetSoft51509.2021.9492534.

[18] M. Riftadi and F. Kuipers, "P4I/O: Intent-based networking with P4", in *Proc. of 2019 IEEE Conference on Network Softwarization (NetSoft)*, 2019, pp. 438–443. DOI: 10.1109/NETSOFT.2019.8806662.

[19] J. Huang, C. Yang, S. Kou, and Y. Song, "A brief survey and implementation on AI for intent-driven network", in *Proc. of 2022 27th Asia Pacific Conference on Communications (APCC)*, 2022, pp. 413–418. DOI: 10.1109/APCC55198.2022.9943612.

[20] A. Leivadeas and M. Falkner, "VNF placement problem: A multi-tenant intent-based networking approach", in *Proc. of 2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2021, pp. 143–150. DOI: 10.1109/ICIN51074.2021.9385553.

[21] M. Mihaeljans and A. Skrastins, "Network topology-aware service function chaining in software defined network", in *Proc. of 2020 28th Telecommunications Forum (TELFOR)*, 2020, pp. 1–4. DOI: 10.1109/TELFOR51502.2020.9306554.

[22] M. Mihaeljans and A. Skrastins, "Reactive service function path discovery approach in software defined network", in *Proc. of 2021 29th Telecommunications Forum (TELFOR)*, 2021, pp. 1–4. DOI: 10.1109/TELFOR52709.2021.9653356.

[23] M. Mihaeljans and A. Skrastins, "Efficient multipath service function chaining in inter-data center networks", in *Proc. of 2023 31st Telecommunications Forum (TELFOR)*, 2023, pp. 1–4. DOI: 10.1109/TELFOR59449.2023.10372615.

[24] J. Zhang *et al.*, "A conflict resolution scheme in intent-driven network", in *Proc. of 2021 IEEE/CIC International Conference on Communications in China (ICCC)*, 2021, pp. 23–28. DOI: 10.1109/ICCC52777.2021.9580197.

[25] M. Beshley, A. Pryslupskyi, O. Panchenko, and H. Beshley, "SDN/Cloud solutions for intent-based networking", in *Proc. of 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 22–25. DOI: 10.1109/AIACT.2019.8847731.

[26] C. Fernández, A. Cárdenas, S. Giménez, J. Uriol, M. Serón, and C. Giraldo-Rodríguez, "Application of multi-pronged monitoring and intent-based networking to verticals in self-organising networks", in *Proc. of 2022 5th International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2022, pp. 1–10. DOI: 10.1109/CommNet56067.2022.9993854.

[27] M. Mihaeljans and A. Skrastins, "Openthread network density evaluation: Quantitative analysis", in *Proc. of 2023 Symposium on Internet of Things (SIoT)*, 2023, pp. 1–5. DOI: 10.1109/SIoT60039.2023.10390236.

[28] R. Caldelli, P. Castoldi, M. Gharbaoui, B. Martini, M. Matarazzo, and F. Sciarrone, "On helping users in writing network slice intents through NLP and User Profiling", in *Proc. of 2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, 2023, pp. 545–550. DOI: 10.1109/NetSoft57336.2023.10175400.

[29] Y. Njah, A. Leivadeas, J. Violos, and M. Falkner, "Toward intent-based network automation for smart environments: A Healthcare 4.0 use case", *IEEE Access*, vol. 11, pp. 136565–136576, 2023. DOI: 10.1109/ACCESS.2023.3338189.

[30] M. Gharbaoui, B. Martini, and P. Castoldi, "Intent-based networking: Current advances, open challenges, and future directions", in *Proc. of 2023 23rd International Conference on Transparent Optical Networks (ICTON)*, 2023, pp. 1–5. DOI: 10.1109/ICTON59386.2023.10207407.