

### **Copyright Notice**


© 2023 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

Institute of Communication Networks and Computer Engineering  
University of Stuttgart  
Pfaffenwaldring 47, D-70569 Stuttgart, Germany  
Phone: ++49-711-685-68026, Fax: ++49-711-685-67983  
Email: [mail@ikr.uni-stuttgart.de](mailto:mail@ikr.uni-stuttgart.de), <http://www.ikr.uni-stuttgart.de>

---

# Security in Intent-Based Networking: Challenges and Solutions

Ijaz Ahmad\*, Jere Malinen\*, Filippos Christou † , Pawani Porambage\*, Andreas Kirstädter †, Jani Suomalainen\*

\*VTT Technical Research Centre of Finland

{firstname.lastname}@vtt.fi

†Institute of Communication Networks and Computer Engineering (IKR), University of Stuttgart, Germany

{firstname.lastname}@ikr.uni-stuttgart.com

**Abstract**—Intent-Based Networking (IBN) aims to automate administrative and management tasks in future communications networks. By leveraging networking concepts such as network abstractions and data-plane programmability and using artificial intelligence (AI), IBN improves the overall efficiency of communications networks. IBN employs a closed-loop architecture to monitor and optimize real-time network performance, reduce human intervention, and enhance resilience. However, the paradigm and the technological enablers introduce security challenges. This article studies the security gains and challenges in IBN from the aspect of enabling concepts and technologies. Furthermore, the article highlights potential solutions to existing challenges, outlines the standardization efforts, and summarizes the most important research gaps to advance future research in this direction.

**Index Terms**—IBN; Security; IBN Security; 6G; Intents

## I. INTRODUCTION

Intent-Based Networking (IBN) is an emerging paradigm for network configuration, which combines concepts from network abstraction, softwarization, automation, and artificial intelligence [1]. It promises user-friendly, cost-efficient, resilient, and secure configuration by presenting network and security requirements as simple intents that govern complex environments, including 6G and multi-domain networks. However, the paradigm opens new attack paths and exposes network users to risks of sabotage, to denial and stealing of network services, and to disclosure of network owner or user-specific secrets.

Existing surveys on IBN, including [1], [2], have studied challenges and opportunities for different application domains, but have not focused on cybersecurity challenges or solutions. We contribute by analyzing security threats and solutions and by surveying existing research efforts for security within IBN. By identifying open gaps, we prepare paths for future research and standardization efforts. This paper is organized as follows. The forthcoming subsections provide the background on IBN. Section II discusses the benefits of IBN in terms of increasing the network security. Section III provides an overview of the arising security challenges with the implementation and use of the IBN and its concepts. A brief introduction to the standardization activities is provided in Section IV along with important future research directions and the article concludes in Section V.

## A. Background

IBN represents an evolution in the way networks are managed and orchestrated. It is a form of network administration that introduces an extra abstraction layer to automate administrative tasks across a network, often by leveraging artificial intelligence (AI) and machine learning (ML) [1]. The fundamental idea of IBN is to allow network administrators to manage networks in accordance with the “business intent” or the organization’s high-level business objectives. Administrators specify what they want the network to do, and the network will configure itself to meet those demands. For instance, if a company wants to prioritize video conference traffic over other types of traffic, they would communicate this intent to the network, and it would take care of the rest.

The operational workflow of IBN is implemented with a closed-loop architecture. The closed-loop control architecture operates by continuously monitoring the state of the network, comparing the actual state with the desired state, and making necessary adjustments to align the two [3], [4]. This cycle is repeated continuously and automatically, enabling the network to respond to changes in real time and maintain optimal performance. This reduces the need for human intervention in network management tasks, makes the network more resilient, and can also improve service quality.

Due to the increasing complexity of communications networks, the concept of IBN can be extremely useful to avoid mishaps, such as configuration errors resulting in security compromises. Software-Defined Networking (SDN) has already paved the way forward with simplicity through decoupling the network control and data planes, and logically centralizing the network control or intelligence [5]. Comparing IBN with SDN and centralized/traditional networking reveals its unique attributes. Traditional networking relies heavily on manual configurations and doesn’t have inherent abilities for automatic adjustment or configuration. On the other hand, SDN still requires significant human intervention and does not inherently align with business intent. IBN takes networking a step further by introducing AI and ML to automate network configuration and operation based on high-level business objectives, thereby minimizing human intervention, reducing errors, and improving overall network agility and performance.

### B. IBN in Different Fields

The Open Systems Interconnection (OSI) layer upon which intents are implemented can differ depending on the scenario. Business institutions mostly target the application and networking layers. For example, applications, such as video surveillance or Voice over Internet Protocol (VoIP) call centers, can be configured by defining the corresponding application-specific intents. Respectively, network related intents can be issued, e.g., for the creation and management of virtual networks. Beyond these, great interest is shown in the definition of IP-optical intents. With this, network operators wish to simplify the coordinated control of their hardware equipment like IP routers, Optical Cross-Connects (OXC), etc.

Control of transport networks involves the appropriate configuration of networking devices such that client demands and Quality of Service (QoS) requirements are met. Although SDN significantly helped to centralize control in a single logical entity [6], today's Internet requires cooperation between different organizations in a decentralized fashion. Consequently, multi-domain networking has become indispensable for a vast portion of realistic scenarios. Since different organizations participate in the same activity, their intentions become worrisome as they can be malevolent. However, still within the realm of security, additional issues appear, such as those of confidentiality and accountability. Confidentiality, in the sense that only disclosed information is allowed to be shared. Accountability, meaning that a suspicious event can be traced back to the responsible entity.

### C. IBN in 6G

Compared to the previous generations of mobile networks, 6G is leaning towards a more of a platform that offers pervasive connectivity to the physical, digital and human worlds by providing a multitude of communication, and beyond, services. Going beyond the performance-based networking paradigms, 6G networks are expected to consider both performance and value based networking paradigm. Among numerous technological enablers that pave the way towards the 6G journey, IBN is one of the key enabler technologies that facilitate human-to-network interfaces and thus enable management and orchestration functionalities in the network [2]. IBN can adjust to various network configuration techniques and physical layer transmission technologies, catering to the demands of the 6G era. This includes addressing challenges such as extensive connectivity, minimal latency, and exceptionally high bandwidth requirements. Leveraging real-time wireless transmission data, IBN capitalizes on big data and AI capabilities to proactively detect network anomalies and execute strategic enhancements and fault rectifications.

Human-to-network interaction can be associated with numerous requirements, such as supporting multi-stakeholder roles, allowing bidirectional feedback to allow information flows from both human-to-machine and machine-to-human, allowing high-level interfaces to facilitate the integration of business and telco technologies without requiring extensive expertise in the telecom sector, and harmonizing actions with

automated recovery and fault management [7]. In addition to these requirements, the security and trust maintained at the human-to-network interface in IBN are also paramount. These may entail the access control, authentication, authorization, and accountability processes as well as the maintenance of trust matrices. For instance, in [8] an example is provided to utilize AI training models and explain their behavior for security-related actions to bring more transparent decisions for human-machine interaction in IBN life-cycle management.

## II. SECURITY GAINS OF IBN

IBN extends the work of SDN, building upon its foundations to introduce intent abstraction and policy-driven automation. As a result, IBN inherits certain security enhancements from SDN while introducing additional benefits associated with its extended capabilities. Intent-driven security extends the IBN concepts to meet cybersecurity related intents and requirements. Intent-driven security policies provide administrator-friendly layer that abstracts the complexity arising from network and security configurations.

### A. Centralized control

One of the primary benefits of IBN stems from its utilization of a centralized network controller, akin to what is seen with SDN. This centralization significantly reduces the potential for policy collisions and configuration errors [9]. In decentralized networks, administrators would need to individually analyze hundreds, if not thousands, of policy-enforcement devices to ensure consistency and accuracy. With IBN, this cumbersome and error-prone task is eliminated, as the centralized approach consolidates and streamlines policy enforcement and configuration, ensuring a more secure and efficient network setup. Furthermore, centralization of control increases network visibility, which in turn allows administrators to collect data from all network devices. Collected data can be analyzed for anomalies using specified ML models [10]. In the event of suspicious activities or breaches, the system is equipped to identify these anomalies and take corrective action. Moreover, with IBN, network intents can be rapidly composed and dispatched to the translation module. This rapid response capability means that the network can be reconfigured or secured at a pace that far exceeds what a human administrator could achieve, even when equipped with a network-wide control plane [10]. This agility is crucial in today's dynamic threat landscape, ensuring that networks can respond promptly and effectively to any potential security threats.

### B. Automated security configuration

Intent-driven security introduces new capabilities for automation and resilience: By presenting security strategies and requirements as intents, low-level configuration and reconfigurations, implementation, and enforcement of the policies can be left for the responsibility of the network. For example, Ooi et al. [11], [12] described a system designer, called SecurityWeaver, to annotate network service requirements with security demands and then automatically generate secure

network designs. They utilized MITRE attack matrix based knowledge base to present security annotations; to identify adversarial tactics and to include appropriate countermeasures into designs. Chowdhary et al. [13] proposed a framework and unified format to express intent-based security policies to facilitate multi-domain cooperation.

IBN further improves network security through its ability to create automated secure services [14]. This feature carefully considers various application requirements, ranging from latency and throughput to end-to-end (E2E) compatibility and the time it takes for connection creation or teardown. Such automation not only ensures optimal performance but also promotes security by tailoring connections to specific needs, reducing potential vulnerabilities or mismatches. In [15], it is shown that intents can also be used for faster security policy conformance checking. The time to verify the host connection permissions is significantly reduced by using algorithms that process intent lists that detail host connections.

### C. Multi-Domain Coordination

Multi-Domain (MD) IBN has been studied in literature like [16], [17], where an overarching orchestrator is assumed. Such cases fall under centralized control with similar security properties. However, the security perspective changes as the domains begin to differentiate from one another. In [18], the authors designed an end-to-end intent-based service management system for technologically diverse domains, and highlighted the importance of a standardized Northbound Interface (NBI). NBI is used to communicate intents to the deployed framework as well as to receive feedback. For distributed framework coordination, authorization becomes necessary [19]. In [20], a decentralized architecture for multi-domain intent-driven operation is presented, which promises confidentiality and accountability across diverse network operators. The work is extended in [21] with the use of intent Directed Acyclic Graphs (DAGs). As a result, IBN turns out to play a major role in establishing secure multi-domain networking, which we attribute to the extra abstraction layer that enables the community to flexibly rethink and standardize common operations.

## III. SECURITY CHALLENGES OF IBN

IBN makes it possible to smoothly deploy the intents of eligible users on the underlying network infrastructure. According to IETF [22], intents are abstractive, declarative, and vendor agnostic set of rules that can be deployed in the following steps, also presented in Fig. 1, designed as components:

- Intent profiling (or delivery): The first component where the user expresses intents to an IBN system. It must be human friendly and the system must facilitate the user for meaningful intent.
- Intent translation (or compilation): Translating the expressed intent into low-level network configurations.
- Intent resolution: Resolving conflicting intents to avoid network-level challenges such as wrong configurations.

- Intent activation (or installation): Provisioning of the intended services requested by intents. Each intent must be deployed in a manner that other intents are not impacted.
- Intent assurance (or monitoring): The intent system uses the closed-loop architecture To make it sure that the network complies with the intent throughout its life-cycle. In dynamic networks such a wireless networks beyond 5G, proactive and reactive measures must be in place to maintain the network configurations accordingly.

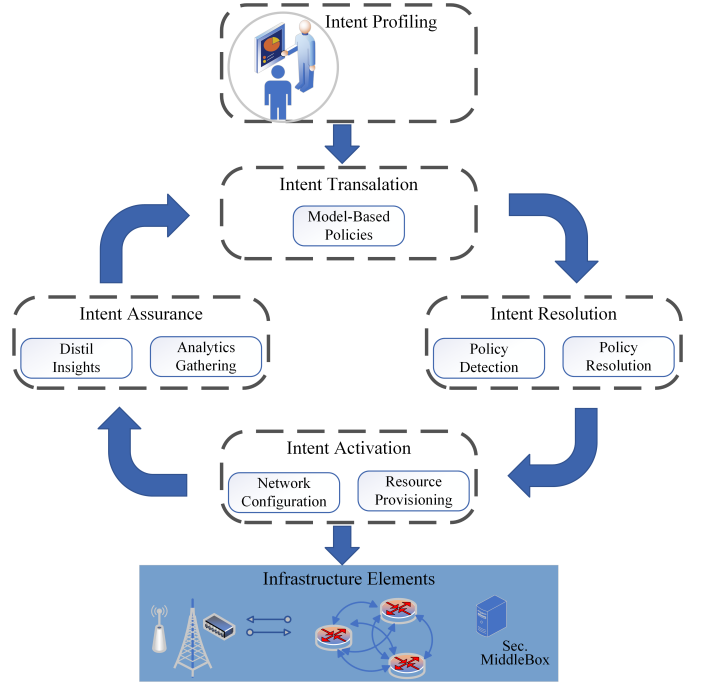


Fig. 1: Components of IBN and interaction among components.

The process and components of IBN are depicted in Fig. 1. It is a cyclic process that starts from the user expressing the intent to the deployment and up until the removal. Each of these steps or components has its own security implications and challenges. Since the process is cyclic, a security lapse at one step or component would exacerbate the security risks of the rest, and bring major challenges in the underlying network infrastructure. In Table I the most prominent security challenges with a brief description, and potential solutions are presented with respect to each step or component of IBN. In the following subsections, we describe various security challenges and potential solutions for different enabling technologies of IBN, which are not contained in the table.

### A. Security threats inherited from SDN

IBN is an evolution of SDN that builds upon its foundation, inheriting both security enhancements and defects associated with SDN. The security challenges inherited from SDN pose significant risks to the overall security of IBN. As with SDN, IBN has a centralized network controller. Centralizing the control plane makes it an attractive target for attackers. A

TABLE I: Security dimensions challenges in IBN with respect to its components

Component	Security Challenge	Brief Description	Potential Solution
Intent profiling	Masquerading attacks	An entity can imitate someone else's identity for malevolent purposes.	Strong authentication and access control procedures, iterative, and verification based intent reading approaches to avoid miss-configurations.
	Miss-configurations due to wrong intent reading	AI-assisted interpretation of intents using Large Language Models (LLMs) can provide inconsistent and fault results.	Confirm validity with rigorous iterative procedures or a strict and deterministic intent language.
	Underskilled personnel	IBN ease-of-use might lead to the employment of undereducated personnel, which can fail to solve problems in corner cases.	Provide education of employees and a simplified and human friendly recording of intents.
	Too coarse-grained control	Decisions, made at a higher level of abstraction, are more keen on overlooking important details and potential risks	Interface support for low-level intents or intent constraints
Intent translation	Complexity exploitation	Complicated intents can create loopholes during translation	Intent verification and beta version deployment can help avoid translation-related challenges.
Intent resolution	Security policy conflicts	Existing intent resolution techniques do not count the possibility security-policy conflicts among stakeholders sharing same underlying network infrastructure	Leveraging network slicing where different user-groups are allocated different virtual instances of the network.
	Deadlock between intents	In case of multiple intents, one intent might allocate the resources needed by another and vice versa	Serial processing of the intents
Intent activation	DoS, DDoS attacks	IBN controllers are centralized, attracting more attacks	Distributing IBN functions and separating from network controllers.
	Erratic state	IBN can introduce further control signal latency due to the extra abstraction layer, which, especially in distributed systems, will lead to slower convergence and inconsistent states.	Opt for fast algorithms and implementations.
Intent assurance	Dynamicity induced vulnerability	Wireless networks are highly dynamic where changes in the network may require quick loop-back to intent resolution, resulting in never ending circles.	AI-based predictive analysis of intent, policy changes, as well as the network states.

successful breach can lead to catastrophic consequences, as the attacker could take control of the entire network. An example of a control plane threat is SDN teleportation. This allows attackers to implicitly gain information about the underlying network via malicious path updates or pass information around via out-of-band forwarding without triggering critical safety functions on the data plane [23].

Another inherited challenge is the vulnerability to denial-of-service (DoS) attacks [5] and the presence of a single point of failure, which can result in the loss of service availability to the IBN controller. A single point of failure also means that unauthorized access to the control plane can have detrimental effects on network security. It allows attackers to exploit sensitive information or tamper with critical network functionalities potentially causing network-wide damage. Furthermore, since SDN controllers are essentially software applications, they are vulnerable to traditional software security issues like buffer overflows, code injection, and other similar vulnerabilities.

SDN networks have been demonstrated vulnerable against fingerprinting attacks [24], [25]. By following the response times or control traffic, adversaries are able to recognize SDN applications that run in SDN controllers. The information leaking enabling these side-channel threats are difficult to prevent as potential mitigations, such as constant response times, would impact control performance.

Finally, the overall treatment against SDN vulnerabilities from the IBN perspective is very much related to the given architecture. Should the IBN framework and the SDN controller be collocated into the same logical entity with a monolithic implementation, like in Fig. 2a, then all issues must be dealt

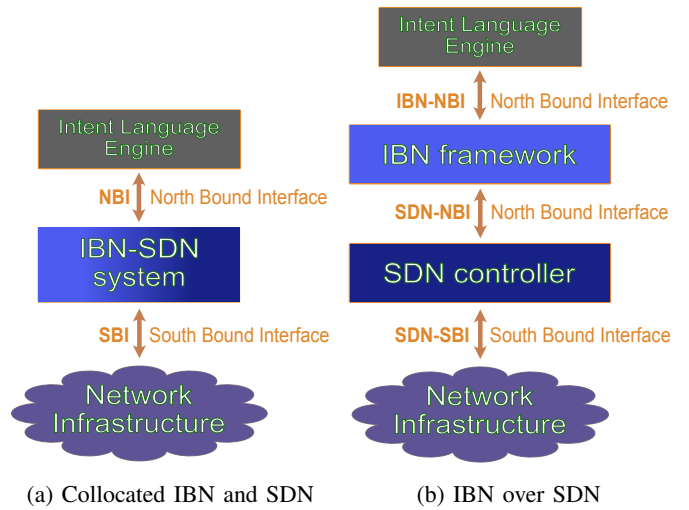


Fig. 2: IBN and SDN co-existing architectures

jointly. But if a more modular architecture is deployed, where the IBN framework is positioned on top of the SDN controller like in Fig. 2b, then the clear boundaries enable a more productive settlement, where different teams can focus on their field of work. As a result, developing an intent-driven solution should not invoke direct concerns regarding the security of the SDN controller, since the two are decoupled.

### B. Security threats related to ML/AI aspects of IBN

The absence of established best practices for the design, development, and deployment of AI-enabled systems presents

a range of significant challenges. These challenges can potentially introduce new vulnerabilities and amplify existing threats, posing serious risks to the integrity and security of such systems [26]. The potential security threats related to ETSI ZSM ML/AI are analyzed in [27] and [28], and mitigation methods are further explored in [29]. These can be categorized to training attacks and inference attacks.

Training attacks involve attackers manipulating the learning process by inserting adversarial data samples or altering specific data points within the training dataset. This is also known as data poisoning. Insufficient guidelines for handling and curating training data can lead to data poisoning. This, in turn, can result in the corruption of AI-enabled systems, causing them to malfunction and provide inaccurate or harmful outputs. Without proper data quality control measures, AI models can learn from tainted data, leading to compromised performance and undesirable consequences. This can appear as incorrect intent translation, causing configuration errors throughout the network. Furthermore, inadequate security measures during the development phase can lead to the insertion of backdoors in pre-trained AI models [30]. These hidden vulnerabilities can be exploited to compromise the system's behavior, allowing unauthorized access or control. Such vulnerabilities can remain inactive until triggered by specific inputs, making them difficult to detect and mitigate.

Inference attacks [31] target machine learning models during their inference phase, which is when the model makes predictions or classifications on new, unseen data. Specifically, attackers aim to exploit the model to extract information about the underlying training data or the model itself without necessarily having direct access to this data. Inference attacks include evasion attacks, model stealing attacks, and data extraction attacks. Evasion attacks involve adversaries strategically altering input samples to mislead a deployed model during its inference phase. Model stealing attacks are carried out by attackers who aim to replicate the capabilities of a targeted model without having direct knowledge of it [32]–[34]. Data extraction attacks involve attackers capable of querying a given model and trying to deduce its training dataset. Two primary forms of data extraction attacks are membership inference attacks and model inversion attacks. The former aims to ascertain if a given sample was part of the model's training data, while the latter seeks to deduce input samples based on model predictions. These attacks not only threaten model confidentiality but can be particularly damaging when the data in question is of sensitive nature.

Another aspect of modern AI that is vertical to security is explainability [35]. Explainable Artificial Intelligence (XAI) refers to the field of research and development that focuses on creating AI systems that can provide understandable and transparent explanations for their decisions and actions [36]. Explainability can contribute to the evaluation of the reliability of an AI system, as the decision-making process and misleading outputs can be assessed. Explainable and reliable AI systems promote trust, which is a crucial factor for the seamless operation of AI technologies. ML-assisted IBN frameworks

must embrace XAI such that critical situations are avoided.

#### IV. STANDARDIZATION ACTIVITIES AND FUTURE RESEARCH DIRECTIONS

The Open Networking Foundation (ONF) [37] started discussions on IBN in 2015. The intent framework was released as a part of the ONOS project. The European Telecommunications Standards Institute (ETSI) GS ENI (Experiential Networked Intelligence) (002, 003, 004, 005), The 3rd Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU) also have started their own efforts towards standardization of IBN. One notable standardization effort is the work being done by the Internet Engineering Task Force (IETF) on Service Assurance in Intent-based Networking (SAIN) [38], [39]. SAIN proposes a general framework for closed-loop automation in service assurance, which involves monitoring the health levels of different subservices of a network service. This standardization effort is aimed at ensuring the reliability and performance of intent-based networks. The International Research Task Force (IRTF) has also been involved in standardization efforts related to IBN [40] and has provided specific definitions of intent that are tailored to their respective core technologies. Finally, the work in [41] discusses the lack of progress in intent-based standardization, based on which [42] identifies advances in natural language processing (NLP) as a potential catalyst for adopting intent-based interfaces. Overall, standardization activities should grow in important research areas of IBN that need to be improved from the security point of view.

#### V. CONCLUSIONS

The role of IBN will increase in the next generations of communications networks, mainly in 6G, due to the increasing complexity of such an ecosystem. IBN meets the requirements of future networks in minimizing complexity in managing and administrating future networks. However, adopting IBN in heterogeneous multi-domain networks presents novel challenges, such as trust, sovereignty, interoperability, and security, which warrant further exploration and research. This article highlights the main security gains of IBN, discusses the main challenges with potential solutions, and provides future research directions in this area.

#### ACKNOWLEDGMENT

This work was supported by the following projects: Hexa-X-II (Grant Agreement no. 101095759), funded by European Union through HORIZON-JU-SNS-2022 call; SUNSET-6G, funded by Business Finland; XcARet, funded by Academy of Finland; and AI-NET-ANTILLAS, funded by Business Finland and BMBF.

#### REFERENCES

- [1] A. Leivadadas and M. Falkner, "A survey on intent-based networking," *IEEE Communications Surveys Tutorials*, vol. 25, no. 1, pp. 625–655, 2023.
- [2] Y. Wei, M. Peng, and Y. Liu, "Intent-based networks for 6g: Insights and challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 270–280, 2020.

- [3] ETSI, “Experiential networked intelligence (eni); overview of prominent control loop architectures,” 2021.
- [4] ETSI, “Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers,” 2021.
- [5] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, “Security in software defined networks: A survey,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.
- [6] S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, “Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects,” *IEEE Access*, vol. 10, pp. 70850–70901, 2022.
- [7] P. Szilágyi, “I2bn: Intelligent intent based networks,” *Journal of ICT Standardization*, pp. 159–200, 2021.
- [8] P. Porambage, J. Pinola, Y. Rumesch, C. Tao, and J. Huusko, “Xcaret: Xai based green security architecture for resilient open radio access networks in 6g,” in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023, pp. 699–704.
- [9] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, “Towards software defined cognitive networking,” in *2015 7th international conference on new technologies, mobility and security (NTMS)*. IEEE, 2015, pp. 1–5.
- [10] J. D. Rivera, T. Ahmed Khan, W. Akbar, A. Muhammad, A. Mehmood, and W.-C. Song, “Automation of network anomaly detection and mitigation with the use of ibn: A deployment case on koren,” in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 294–299.
- [11] S. E. Ooi, R. Beuran, Y. Tan, T. Kuroda, T. Kuwahara, and N. Fujita, “Secureweaver: Intent-driven secure system designer,” in *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 2022, pp. 107–116.
- [12] S. E. Ooi, R. Beuran, T. Kuroda, T. Kuwahara, R. Hotchi, N. Fujita, and Y. Tan, “Intent-driven secure system design: Methodology and implementation,” *Computers & Security*, vol. 124, p. 102955, 2023.
- [13] A. Chowdhary, A. Sabur, N. Vadnere, and D. Huang, “Intent-driven security policy management for software-defined systems,” *IEEE Transactions on Network and Service Management*, 2022.
- [14] T. Szyrkowiec, M. Santuari, M. Chamania, D. Siracusa, A. Autenrieth, V. Lopez, J. Cho, and W. Kellerer, “Automatic intent-based secure service creation through a multilayer SDN network orchestration,” *Journal of Optical Communications and Networking*, vol. 10, 2018.
- [15] N. Herbaut, C. Correa, J. Robin, and R. Mazo, “Sdn intent-based conformance checking: application to security policies,” in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, 2021, pp. 181–185.
- [16] L. Velasco, M. Signorelli, O. G. De Dios, C. Papagianni, R. Bifulco, J. J. V. Olmos, S. Pryor, G. Carrozzo, J. Schulz-Zander, M. Bennis, R. Martinez, F. Cugini, C. Salvadori, V. Lefebvre, L. Valcarengi, and M. Ruiz, “End-to-end intent-based networking,” *IEEE Communications Magazine*, vol. 59, no. 10, pp. 106–112, 2021.
- [17] M. Xie, P. H. Gomes, J. Niemöller, and J. P. Waldemar, “Intent-driven management for multi-vertical end-to-end network slicing services,” in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 1285–1291.
- [18] G. Davoli, W. Cerroni, S. Tomovic, C. Buratti, C. Contoli, and F. Callegati, “Intent-based service management for heterogeneous software-defined infrastructure domains,” *International Journal of Network Management*, vol. 29, 2018.
- [19] S. Arezoumand, K. Dzevaroska, H. Bannazadeh, and A. Leon-Garcia, “Md-ids: Multi-domain intent-driven networking in software-defined infrastructures,” in *2017 13th International Conference on Network and Service Management (CNSM)*, 2017, pp. 1–7.
- [20] F. Christou, “Decentralized intent-driven coordination of multi-domain ip-optical networks,” in *2022 18th International Conference on Network and Service Management (CNSM)*, 2022, pp. 359–363.
- [21] F. Christou and A. Kirstaedter, “Grooming connectivity intents in ip-optical networks using directed acyclic graphs,” in *Photonic Networks: 24th ITG-Symposium*, 2023, pp. 1–4.
- [22] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, “Intent-based networking-concepts and definitions,” *IRTF draft work-in-progress*, 2020.
- [23] K. Thimmaraju, L. Schiff, and S. Schmid, “Outsmarting network security with sdn teleportation,” in *2017 IEEE European Symposium on Security and Privacy (EuroSP)*, 2017, pp. 563–578.
- [24] R. Bifulco, H. Cui, G. O. Karame, and F. Klaedtke, “Fingerprinting software-defined networks,” in *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*. IEEE, 2015, pp. 453–459.
- [25] J. Cao, Z. Yang, K. Sun, Q. Li, M. Xu, and P. Han, “Fingerprinting SDN applications via encrypted control traffic,” in *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, 2019, pp. 501–515.
- [26] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, “Machine learning threatens 5g security,” *IEEE Access*, vol. 8, pp. 190822–190842, 2020.
- [27] ETSI, “Zero-touch network and Service Management (ZSM); General Security Aspects,” *Group Report (GR)*, 2021.
- [28] ETSI, “Securing artificial intelligence (sai); problem statement,” *Group Report (GR)*, 2020.
- [29] ETSI, “Securing Artificial Intelligence (SAI); Mitigation Strategy Report,” 2021.
- [30] S. Sasaki, S. Hidano, T. Uchibayashi, T. Suganuma, M. Hiji, and S. Kiyomoto, “On embedding backdoor in malware detectors using machine learning,” in *2019 17th International Conference on Privacy, Security and Trust (PST)*, 2019, pp. 1–5.
- [31] D. Ye, S. Shen, T. Zhu, B. Liu, and W. Zhou, “One parameter defense—defending against data inference attacks via differential privacy,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1466–1480, 2022.
- [32] S. J. Oh, B. Schiele, and M. Fritz, *Towards Reverse-Engineering Black-Box Neural Networks*. Cham: Springer International Publishing, 2019, pp. 121–144.
- [33] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, “Stealing machine learning models via prediction APIs,” in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, pp. 601–618.
- [34] D. Oliynyk, R. Mayer, and A. Rauber, “I know what you trained last summer: A survey on stealing machine learning models and defences,” *ACM Computing Surveys*, 2023.
- [35] M. Choraś, M. Pawlicki, D. Puchalski, and R. Kozik, “Machine learning – the results are not the only thing that matters! what about security, explainability and fairness?” in *Computational Science – ICCS 2020*, V. V. Krzhizhanovskaya, G. Závodszyk, M. H. Lees, J. J. Dongarra, P. M. A. Sloot, S. Brissos, and J. Teixeira, Eds. Cham: Springer International Publishing, 2020, pp. 615–628.
- [36] A. Arrieta, N. Díaz-Rodríguez, A. Bennetot, S. Tabik, A. Barbedo, S. García, S. Gil-Lopez, D. Molina, R. Benjamins, R. Chatila, and F. Herrera, “Explainable artificial intelligence (xai): concepts, taxonomies, opportunities and challenges toward responsible ai,” *Information Fusion*, vol. 58, pp. 82–115, 2020.
- [37] Open Networking Foundation (ONF), “Intent-Based Networking,” <https://opennetworking.org/news-and-events/blog/intent-based-networking/>, 2015, accessed: 2023-08-22.
- [38] K. Edeline, T. Carlisi, J. Iurman, B. Claise, and B. Donnet, “Towards a closed-looped automation for service assurance with the dxagent,” in *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*, 2022, pp. 67–72.
- [39] B. Claise, J. Quilbeuf, D. Lopez, D. Voyer, and T. Arumugam, “Service Assurance for Intent-Based Networking Architecture,” RFC 9417, Jul. 2023. [Online]. Available: <https://www.rfc-editor.org/info/rfc9417>
- [40] C. Li, O. Havel, A. Olariu, P. Martínez-Julia, J. C. Nobre, and D. Lopez, “Intent Classification,” RFC 9316, Oct. 2022. [Online]. Available: <https://www.rfc-editor.org/info/rfc9316>
- [41] E. Zeydan and Y. Turk, “Recent advances in intent-based networking: A survey,” in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.
- [42] J. Mcnamara, D. Camps-Mur, M. Goodarzi, H. Frank, L. Chinchilla-Romero, F. Cañellas, A. Fernández-Fernández, and S. Yan, “Nlp powered intent based network management for private 5g networks,” *IEEE Access*, vol. 11, pp. 36642–36657, 2023.