# Artificial Intelligence Techniques for Information Security in 5G IoT Environments

Ivan Petrov, Toni Janevski

***Abstract* — The development of the telecommunication networks observed in present and future time is impressive. Today we witness rapid implementation of 5G networks. We can say that this actually is the moment when (artificial intelligence) AI enters at small door but in the beyond 5G world it is expected to have the prime role in smart operation, management and maintenance of non-software defined networking (SDN), network function virtualization (NFV) and especially at SDN and NFV aware networks. Number of standardization body's and work groups are focused in a way to create a framework that will define the future use of AI and security standards necessary to exist in order to create health environment for the next generation telecommunication infrastructure. In the wireless world AI/Machine learning (ML) has great potential to shake the way we operate and to become foundation of the transformation that leads to the next industrial revolution. Network virtualization gives flexibility and freedom of the telco operators to choose the hardware and network topology they need for AI/ML platforms and big data sets. 5G and IoT create positive environment for AI and ML development and usage. As the network requirements are developed and the number of the users raises, gains are expected to grow with the number of variables and the interactions among them so it becomes impossible to relay on humans to control the network for increased number of variables and this is why AI with ML and automation become beneficial and necessity to run the future networks. AI generally is defined as capacity of mind or ability to acquire and apply knowledge and skills while ML is defined as learning that does not require explicit programming. Combined usage of AI and ML can optimize almost any component of the wireless network, this does not mean that it should be used everywhere mainly because at the end of the day the cost benefit analysis of its usage must be positive. Smart operation, management and infrastructure maintenance (SOMM) networks are defined as: Intelligent, data driven, integrated and agile. Today AI is introduced but in future it will represent the network engine. It is interesting to mention that network security must be upgraded because the network will provide services for massive number of IoT devices that will have variety of functions and requests. AI/ML can improve the security services and to be used in order to elevate them at advanced level. In this text we focus our attention at AI/ML and security scenarios defined for IoT in 5G environment.**

***Index Terms* — AI, ML, NGN, security.**

## I. INTRODUCTION

SOMM network has to be intelligent [1] in a meaning that the network can perform management and maintenance in precise and simple way instead of humans and to give predictive judgements on network service failures and optimizations based on big data, AI algorithms and engaged smart devices. This network must be capable to support data sharing, mining, data correlation, machine learning or simply said it must be capable of data convergation form different OS in one unified data model. This understanding actually stands behind the real meaning of Data driven network and when we say Integrated it actually means that this network model must be capable to support the existing and future network frameworks in a way the end to end services to be fulfilled for variety of customers. From all described above it can be concluded that the network has to have service-oriented infrastructure in which different system functions are packed as a service. Taking in consideration what is expected from SOMM one may conclude that its application can be divided in following five categories: smart operation, smart management, smart maintenance, comprehensive management, traditional operation, administration and maintenance.

## II. FUNCTIONAL CHARACTERISTICS OF AI GUIDED NETWORK

It is important the AI guided network to assure end to end service provisioning in a variety of scenarios when variety of vendor equipment and domains are engaged. The network must be capable of malfunction complaint prevention and treatment, end to end fault processing and etc. The network must be capable to establish synergy and 5G slice management. Unified orchestration is needed to assure cloud and network services to be deployed at customer demand. When 5G slice management is discussed we have to be aware that it occurs among multi-layer and multi domain networks where number of different technologies are used. Smart network monitoring on the other side includes daily monitoring of the network behavior and service provisioning in end to end manner. Smart maintaining activities usually cover on site activities with help of usage of AI equipment (IoT based devices and etc.). Big data analysis is expected to be engaged when cross layer and cross domain operation and management is requested with help of data collecting, modelling and processing. ITU recommends [1], [2] SDN and NFV aware networks to be managed by SDN orchestrator/ controller and NFV MANO separately or by a unified orchestrator jointly as is presented at Fig. 1.

Published on November 13, 2020.
Ivan Petrov.
(e-mail: ivan.petrov@telekom.mk)
Toni Janevski.
(e-mail: tonij@feit.ukim.edu.mk)

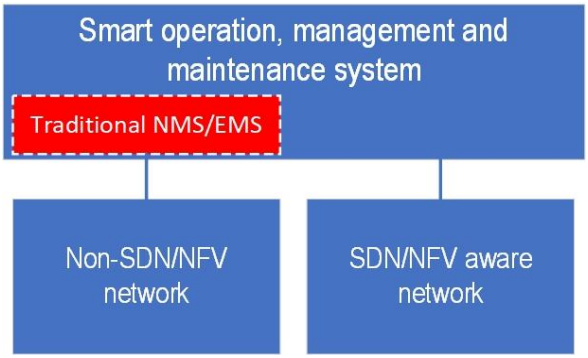



Fig. 1. Top view of smart operation, management, and maintenance system [1].

Layered functional architecture of SOMN is proposed by ITU and presented at Fig. 2. Form Fig. 2 it can be differentiated four main layers that contain sub layer functionalities.

Scenario application layer is recommended to be consisted of five management function sets as smart operation, smart management, smart maintenance, smart comprehensive analysis and traditional B-OSF's.

Management service layer is defined to contain two sub layers as service opening sub layer consisted of service directory and service management and service providing sub layer that includes following set of management functions: SDN/NFV aware orchestration and traditional S-OSF, N-OSF, E-OSF. It is defined that in SDN/NFV aware orchestration and the traditional one, AI assists in form of mathematical analysis and prediction in machine learning used to meet the management needs.

Data convergence and management layer is consisted of two sub layers. Data management sub layer formed by data lifecycle management and data security management sub layers while data convergence sub layer is consisted of data acquisition, data processing, data storage and traditional N-OSF and E-OSFs management function sets.

Infrastructure management layer has function of managing the common infrastructure of OSs. It is consisted of smart infrastructure maintenance and infrastructure monitoring sub layers.

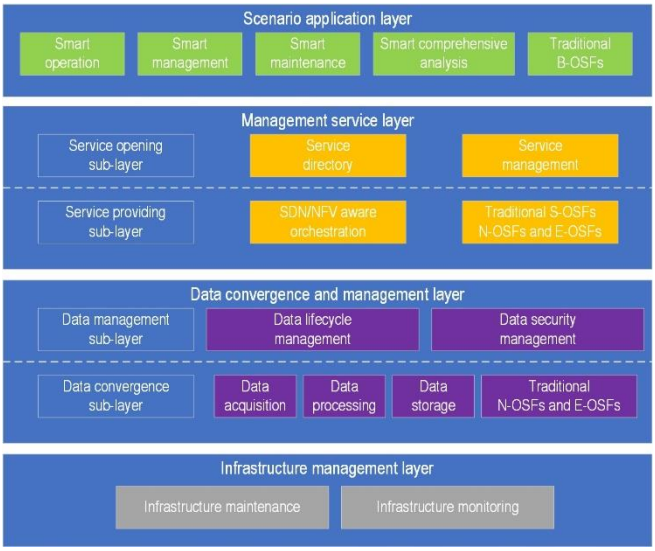



Fig. 2. Layered functional architecture of SOMM with sub functions.

## III. MACHINE LEARNING IN FUTURE NETWORKS

AI is directly corelated with machine learning (ML). As is specified in [2] number of architectural requirements and specific architectural components must be satisfied in order ML to be enabled in future network architectures. Machine learning actually represents processes that enable the system to understand data and to gain knowledge from it without to be explicitly programmed in order to realize complicated tasks like detection of characteristics or prediction of behavior. It is requested general requirements and mechanisms in IP networks to be applied as recommended in [3], [4]. This security implementations must be fulfilled in order to prevent unauthorized access, data licking with implementation of mechanisms regarding authentication and authorization, external attack protection and etc.

At Fig. 3 is presented ITU recommendation of high-level architectural components where ML pipeline is consisted of a set of logical nodes each with different functionalities that can be combined to form a machine learning application in the network. SRC represent the source of data that is used as an input in the pipeline. C represents the collector that is responsible for collecting data form one or more SCR nodes. The preprocessor PP is responsible for cleaning the data and performs preprocessing operations in order to prepare the data for the ML model to consume it. Policy node (P) enables the application of polices to the output of the model node. The distributor D is responsible for identifying the sink(s) and distributes the output of the M node to the corresponding SINKs. SINK represents node defined as a target of the ML output. MLFO is logical node with functionalities that manage and orchestrate the nodes of ML pipelines based on ML. ML Intent represent declarative description used to specify ML application it does not specify technology specific network functions to be used in ML application and provides a basis for mapping ML applications to diverse technology specific network functions. ML sandbox represents isolated domain which allows the hosting of separate ML pipelines to train test and evaluate them before deploying them in the real network. High level architecture is described in details in [2].

Framework for evaluating the intelligence levels of future networks including IMT-2020 are introduced in [5] where are recommended developing trends of network intelligence, methods of evaluating network intelligence levels and architectural view for evaluating network intelligence levels are presented. It is already defined that AI including ML is considered to be a promising technology to cope with the increasing complexity and to improve the performance of future networks including IMT-2020. As networks become more and more intelligent, it is important to adopt a standard method for evaluating network intelligence levels.

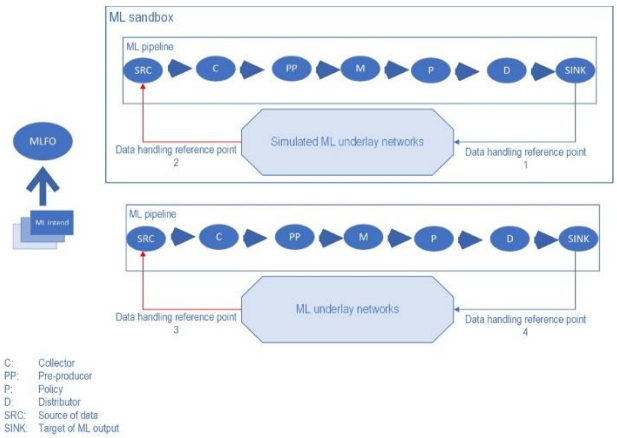



Fig. 3. High level architectural components.

A standard method for evaluating network intelligence levels has the following implications [5]. It provides an evaluation basis for measuring the intelligence levels of a network and of its components; It helps the industry to reach a consensual and unified understanding of network intelligence concepts; It provides a reference for industry supervisors to formulate relevant strategies and development planning of future networks including IMT-2020 in various countries; It provides a decision mechanism to operators, equipment vendors and other network industry participants for planning of network technology features and products' roadmaps.

Five generally applicable dimensions are recommended to be used for evaluating of the network intelligence levels.

As is presented at Fig. 4 the dimensions are: Demand mapping, Data collection, Analysis, Decisions and Action implementation.

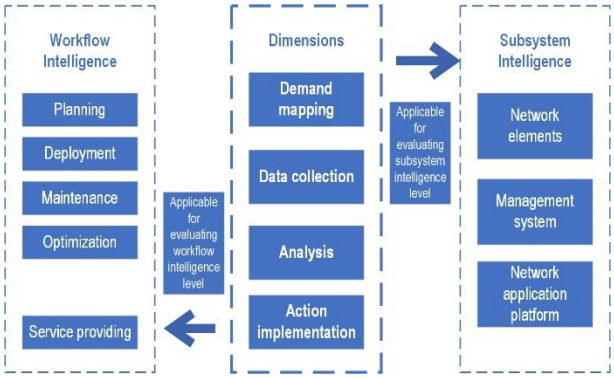



Fig. 4. Dimensions for evaluating network intelligence levels.

The concept of ML is upgraded in [6] where several newly defined handling architectural components are introduced, as ML metadata store the Data models (DM) usable in the network for ML application. Example of upgraded high level architecture components of the data handling framework is presented at Fig. 5. DM may have companion API specifications denoted as API-g. API-g is an architectural component which represent the API for a machine learning DM to be used in a ML overlay. DBr-UP maps the API-g to the API-s which is specific to ML underlay networks. The API-s is an architectural component which represents the API which has to be used towards corresponding ML underlay networks. API-s is used by DBr-UP, in conjunction with API-g, to map the generic API to the specific APIs of ML underlay networks. The ML data broker user plane (DBr-UP)s is an architectural component which facilitates the use of appropriate API-s towards the ML underlay network functions and maps the incoming data from the ML underlay network functions to the ML, DM used in the ML overlay. The ML database (DB) is an architectural component providing storage support for data used by ML applications. This storage may be used for sharing data between various architectural components of the data handling framework. Additional details of this model are presented in [6]

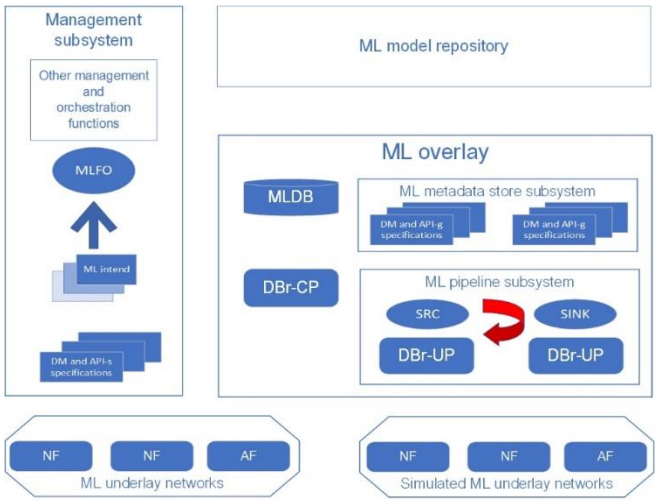



Fig. 5. High level architecture components of the data handling framework.

Form this point of view we can say for sure that initial standards are upgraded at daily basis, statement that can be proved with [7].

Now when are defined the basic concepts of AI and ML we can discuss their usage in 5G and future network. At Fig. 6 we have presented simple example of network optimization achieved with help of AI/ML.

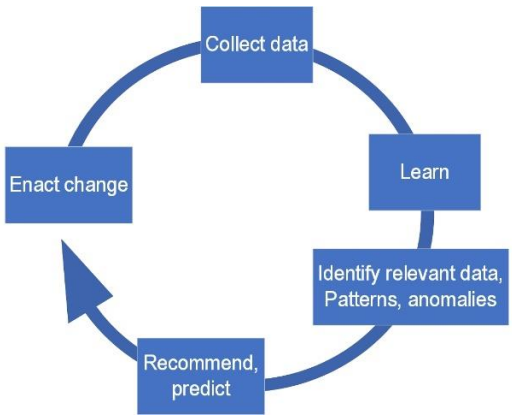



Fig. 6. Network optimization with AI/ML.

If we ask what is the reason of the increased network complexity the answer will contain device types (smartphones, laptops, IoT devices, sensors, cctv, and etc.), applications and use cases, RAN (coexistence and integration across access technologies form 2G up to 5G with included unlicensed bands, mMIMO and beamforming), Core (edge and cloud computing, virtualization, network slicing), Traffic management (analytics, application level traffic management), Testing and monitoring that includes real time network troubleshooting. If we know what actually increases

the network complexity then we can use AI/ML to improve its performance. Actually, we can use AI/ML to improve any performance and financial metric as: Quality of experience, reliability, resource utilization, throughput, latency, per value bit, per cost bit and etc.

## IV. IoT and AI

Today we witness that IoT technology has been shifted to creating value through analytics, sensing, gains from established connections and etc. Regarding the network performance optimization, the AI/ML can be used as essential tool to support IoT applications. IoT applications are generating data collected from various domains and industrial sectors. The data generated provides insights from the environments and applications that generated it. AI techniques provide the framework and tools to go beyond analytics of real time monitoring and automation use cases for IoT and moves to IoT platforms that use concepts from AI and apply them to specific IoT use cases to assure smarter decision-making. AI-enabled IoT applications add a new layer of functionality's and access, creating the next generation of smart homes/buildings, smart vehicles and smart manufacturing by providing intelligent automation, predictive analytics and proactive intervention. The use of AI, swarm intelligence and cognitive technologies together with deep learning techniques for optimizing the IoT services provided by IoT applications in smart environments and collaboration spaces will create solutions capable of transforming industries and professions. The IoT can be characterized as a cyber physical system (CPS). A CPS may be as simple as an individual device or a CPS can consist of one or more cyber-physical devices that form a system or can be a SoS, consisting of multiple systems that consist of multiple devices. This pattern is recursive and depends on one's perspective. CPS must contain the decision flow together with at least one of the flows of information or action. The information flow represents digitally the measurement of the physical state of the physical world, while the action flow impacts the physical state of the physical world. This allows collaborations from small and medium scale up to city/nation/world scale.

CPSs enable the physical world to merge with the virtual world by integrating computation and physical processes. A CPS facilitates tight integration between computation, communication, and control in its operation and interactions with the environment in which it's deployed.

## V. Security in IoT and AI

IoT promises to integrate and connect everyday objects such as sensors, actuators and other physical objects to the Internet providing state-of-the-art intelligent services. Security issues such as jamming, spoofing, denial of services, eavesdropping, malwares in the form of viruses, Trojans, worms and etc. are a great source of concern when it comes to designing and developing secured IoT systems. They present a variety of potential risks that could be exploited to harm users or to even bring down an entire system via: unauthorized access and misuse of personal information; attacks facilitation on other systems; risks of personal safety.

In IoT are assumed different dimensions since the conventional security mechanisms based on authentication, confidentiality, malware prevention and etc. cannot be directly deployed on IoT devices because of resource scarcity. IoT devices have prohibitively limited resources, battery lifetime, and even network bandwidth to run the traditional compute intensive security mitigation mechanisms. The lack of effective security measures enables malicious parties to access and misuse personal information, collected and transmitted through the IoT devices and network which is a challenge that needs to be urgently tackled. In smart home environment, the more the number of devices connected to the network, the more the vulnerabilities a malicious person could exploit to compromise personal information. Another potential target is the network. Attack on any IoT device can facilitate attacks on the network to which it is connected and with potential to cause attack on several other connected devices. The AI techniques based on machine learning for example, can recognize trends from past experiences and then are able to make predictions. Therefore, security solutions based on AI techniques are expected to react more effectively to new threats than the traditional security approaches. In security, availability of big data means that AI techniques can be exploited to analyze and recognize patterns of security vulnerabilities to prevent such attacks. The ability of IoT based platform to learn from data, to analyze, identify and mitigate security threats is an important feature that every IoT system should incorporate. These techniques are also more accurate in terms of assessment of potential malware threats from large quantity of data. In addition, AI is very suitable to detect and mitigate sophisticated attackers such as advanced persistent threats in which attackers can remain undetected for indefinite period. The security challenges in IoT could range from insufficient authentication, authorization, insecure network services, lack of transport encryption, insecure cloud and edge interfaces, insecure mobile interface, poor security configurability problems, insecure software or firmware and even poor physical security. We should also note that most IoT devices have been developed without taking security into consideration mainly because these devices have limited computational resources to execute security mechanisms.

## VI. Security in future networks

As the network complexity increases the risk to establish trustworthy networking decreases. Future networks beside the technical advantages they offer: increased data speed, decreased latency and services based at these achievements, the general trend is the future network to serve increased number of the users. IoT rapidly increases the number of connections established by these networks and for sure this number will grow with the time.

One of the network priorities is to assure trustworthy networking. Trust is directed relationship between the network elements. This actually means that an identity of a network element must be well defined and afterwards is necessary to check whether the element that is identified is trustworthy or has past predefined security evaluation. If the check is positive then trustworthy communication is

established between the peer network elements [9]. This model is actually presented at Fig. 7. Security is important and has to be at highest level in order to minimize and to protected the network from external attacks and threats. One of the approaches is to create isolated network form the external networks, meaning that the insulated network enforces appropriate trust policies and procedures that will keep the network protected. There are number of proposed solutions and one of the approaches is to dived the network in trust domains that are connected with well-defined interfaces. This model assures intra communication inside the trust domain that can be done without security protection. This type of communication is defined as mutual trust relationship [9]. Inter-domain communication between the network domain and the external network is managed by trustworthy interface and its relationship is defined as asymmetric trust relationship. The trust-centric network domain represents an abstraction of a network in which all members have a mutual trust relationship defined by specific properties as functional and administrative features. This trust centric network domain assures trustworthy communication by performing domain administration, membership management, access and delivery control functionalities. In order this communication to be established there are number of high level and functional requirements that has to be fulfilled. At Fig. 8 is presented extended representation of the trust model for trustworthy networking.

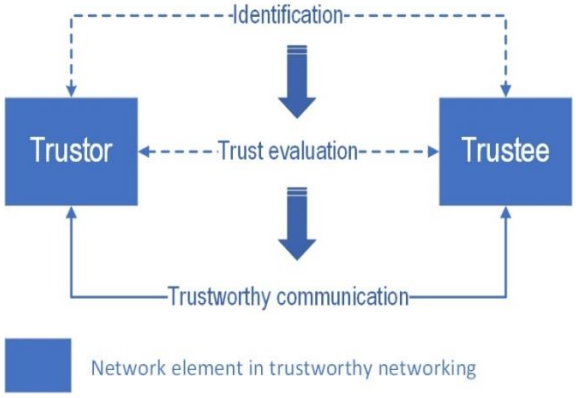



Fig. 7. Model of trustworthy networking.

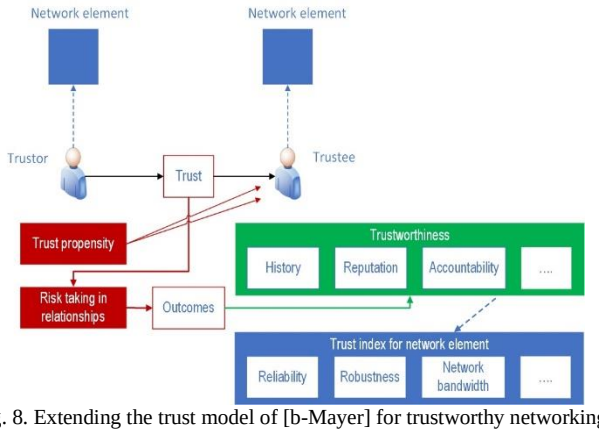



Fig. 8. Extending the trust model of [b-Mayer] for trustworthy networking.

Cryptographic techniques are widely studied for authentication and may fall short of the desired performance in many emerging scenarios of 5G-and-beyond wireless networks [10]. The fundamental weaknesses of conventional cryptography techniques are the increasing latencies, communication and computation overheads for achieving better security performance, which are extremely undesirable for delay-sensitive communications and resource-constraint devices.

Appropriate key management procedures are necessary for the conventional cryptographic techniques, and cooperation among multiple entities is required for both ring and group signature, leading to excessive latencies and significant communication overhead. Due to the inherent features of communicating devices, detecting compromised security keys cannot be readily achieved by conventional digital credentials-based techniques [10]. Physical layer authentication provides an alternative approach of validating a device by exploiting the communication link, device, and location-related attributes, as exemplified by channel impulse response [11]-[16]. There are number of challenges for existing physical layer authentication. This is only one desirable engagement of intelligent authentication approaches with help of machine learning to address the above challenges for security enhancement and more efficient management in 5G-and-beyond networks, as presented in [17]–[19]. Novel models of trustworthy communication supported by AI and ML will be subject of deep analysis and further work of the standardization bodies. Number of learning models can be used to assure security in NGN that will take in consideration exponential growth of the network complexity. Parametric learning, non-parametric, supervised learning, unsupervised learning, reinforcement learning models are only few of them that can be used.

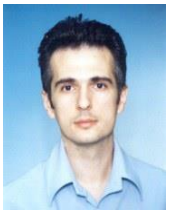
## VII. Conclusion

In this paper we have exposed our view of future development of beyond 5G networks. New technologies as 5G NR, URLLC, mMIMO have well defined role in the network transformation while AI/ML is at entry level in the NGN in a way that shifts the entire network infrastructure and the users of distributed architecture, automation and virtualization. The convergence of AI/ML in operations is driven by increased network complexity with aim to improve the utilization and customer satisfaction. AI/ML and IoT are creating dynamic network environment. This change will take some time and eventually will result with creation of dynamic and agile network that will learn autonomously to optimize its performance, it will use its resources efficiently, will optimize itself in real time, will assure full power of the 5G benefits, will improve support for IoT, will strengthen security and at the end will generate increased revenue. We have overviewed basic recommendations that NGN has to obey in order to implement AI/ML techniques and how IoT will impact the future network development and security. At the end we can conclude that AI/ML will shape the future network development and services.

## REFERENCES

[1] Recommendation ITU-T M.3041 "Framework of smart operation, management and maintenance" – Series M: Telecommunication management including TMN and network maintenance – Telecommunications management network - 02.2020.
[2] Recommendation ITU-T Y.3172 "Architectural framework for machine learning in future networks including IMT-2020" – Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-06.2019.
[3] Recommendation ITU-T Y.2701 "Security requirements for NGN release 1" Series Y: Global information infrastructure, internet protocol aspects and next generation networks, Next Generation Networks-Security.
[4] Recommendation ITU-T Y.3101 "Requirements of the IMT-2000 network" - Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-01.2018.
[5] Recommendation ITU-T Y.3173 "Framework for evaluating intelligence levels of future networks including IMT-2020" - Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-02.2020
[6] Recommendation ITU-T Y.3174 "Framework for evaluating intelligence levels of future networks including IMT-2020" - Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-02.2020.
[7] ITU-T Y-series Recommendations – Supplement 59 "ITU-T Y.3100-series – IMT-2020 standardization roadmap" - Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-03.2020.
[8] ITU report on AI and IoT in Security Aspects "Artificial Intelligence (AI) for Development series" 07.2018
[9] Recommendation ITU-T Y.3053 "Framework of trustworthy networking with trust-centric network domains" - Series Y: Global information infrastructure, internet protocol aspects, next generation networks, internet of things and smart cities, Future networks-01.2018
[10] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," IEEE Wireless Commun. Mag., vol. 24, no. 2, 2018, pp. 98-105.
[11] H. Fang, X. Wang, and L. Hanzo, "Learning-aided Physical Layer Authentication as an Intelligent Process," IEEE Trans. Commun., vol. 67, no. 3, 2019, pp. 2260-2273.
[12] Sang-Hyun Park, "D3.1 - Intermediate Report On Enhanced 5g Radio Access Technologies," Ref. Ares (2019)6421524 - 17/10/2019.
[13] W. Hou, X. Wang, J. Chouinard, and A. Refaey, "Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets," IEEE Trans. Commun., vol. 62, no. 5, 2014, pp. 1658-1667.
[14] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless Physical Layer Identification: Modeling and Validation," IEEE Trans. Inf. Forensics Security, vol. 11, no. 9, 2016, pp. 2091-2109.
[15] Y. Liu, H. H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," IEEE Commun. Surveys Tuts., vol. 19, no. 1, 2017, pp. 347-376.
[16] S. Tomasin, "Analysis of Channel-based User Authentication by Key-less and Key-based approaches," IEEE Trans.Wireless Commun., vol. 17, no. 9, 2018, pp. 5700-5712.
[17] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques based on Machine Learning: How do IoT Devices use AI to Enhance Security?" IEEE Signal Process. Mag., vol. 35, no. 5, 2018, pp. 41-49.
[18] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet Things J., vol. 5, no. 6, 2018, pp. 4829-4842.
[19] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine Learning for Wireless Connectivity and Security of Cellular-Connected.

**Ivan Petrov** is with Makedonski Telekom Skopje, Macedonia – mobile and fix network telecom operator member of Deutsche Telekom Group for almost 15 years, currently he holds position of Senior Project Manager in Business Operation Unit. He received his Dipl.Ing., M.Sc. and Ph.D. from the Faculty of Electrical Engineering, Ss. Cyril and Methodius University in Skopje, in 2005 and 2009 and 2017 respectively. From 2018 he is with University American College Skopje where he has a position of Assistant professor in the field of Telecommunications and Computer Science subjects. His research interests include transport protocols and cross-layer optimization techniques in heterogeneous wireless IP networks.



**Toni Janevski, Ph.D.**, is a Full Professor at the Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, Skopje, Macedonia. He received his Dipl. Ing., M.Sc. and Ph.D. degrees in electrical engineering all from Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University in Skopje, in 1996, 1999 and 2001, respectively. In the past, during 1996-1999 he has worked for the Macedonian mobile operator Mobimak (currently T-Mobile, Macedonia), contributing to the planning, dimensioning and implementation of the first mobile network in Macedonia. From 1999 he is with Faculty of Electrical Engineering and Information Technologies in Skopje. In 2001 he has conducted research in optical communications at IBM T. J. Watson Research Center, New York. During 2005-2008 he was an elected member of the Commission of the Agency for Electronic Communications (AEC) of the Republic of Macedonia. During the periods 2008-2012 and 2012-2016 he is an elected member of the Senate of the Ss. Cyril and Methodius University in Skopje. In 2009 he has established Macedonian ITU (International Telecommunication Union) Centre of Excellence (CoE) as part of the Europe's CoE network, and serves as its head/coordinator since than. He is the author of the book titled "Traffic Analysis and Design of Wireless IP Networks", which is published in 2003 by Artech House Inc, USA. Also, he is the author of the book "Switching and Routing", written in Macedonian language, published in September 2011 by the Ss. Cyril and Methodius University in Skopje. In 2012 he has won "Goce Delchev" award, the highest award for science in the Republic of Macedonia (can be received once in a lifetime). Also, he received Best Scientists Award of the Ss. Cyril and Methodius University in Skopje for 2013 (can be received once for a lifetime). In April 2014 has appeared his second worldwide book titled "NGN Architectures, Protocols and Services", published by John Wiley & Sons, UK. In July 2015 appeared his book "Internet Technologies", written in Macedonian language, published by the Ss. Cyril and Methodius University in Skopje. He is also author of the book "Internet Technologies for Fixed and Mobile Networks", published in November 2015 by Artech House, USA. Further, in April 2019, he has published the book "QoS for Fixed and Mobile Ultra-Broadband", John Wiley & Sons (Wiley – IEEE Press series), UK. He has published numerous research papers and has led several research and application projects in the area of Internet technologies and mobile and wireless networks. Also, he has tutored and coordinated many international courses in the ITU Academy. He is a Senior Member of IEEE since 2005. He is currently a member from Europe region in the ITU's global GCBI (Group on Capacity Building Initiatives), in the term 2018-2022. His interests include Internet Technologies, Mobile, Wireless and Multimedia Networks and Services, Traffic Engineering, Quality of Service, Design and Modeling of Telecommunication Networks, Next Generation Networks, Cloud Computing, and Future Networks.