IOT-NETWORKS IN GROUP BASED MODEL

[1] V. VANEESWARI, [2] S. SELVAKUMARI, [3]S.SUBATHRA

[1][2][3]ASSISTANT PROFESSOR IN COMPUTER SCIENCE,

Dhanalakshmi Srinivasan College of Arts and Science for Women (Autonomous)

Perambalur

ABSTRACT

The Internet of Things (IoT), hailed because the enabler of subsequent technological revolution, would require ubiquitous connectivity, context-aware and dynamic service mobility, and extreme security through the wireless network infrastructure. Artificial Intelligence (AI), thus, will play a serious role within the underlying network infrastructure. However, variety of challenges will Surface when using AI's concepts, tools and methods wireless networks employed by IoT . During this article, the most challenges in using AI within the wireless network infrastructure that facilitate end-to-end IoT communication are highlighted with potential generalized solution and future research directions.

I. INTRODUCTION

The Internet of Things (IoT), the word was first coined by Kevin Ashton.In this is an extension of the network connection devices, like actuators, sensors and mobile devices, enabled to interact and communicate among themselves, and may be controlled or monitored remotely. IoT, hailed because the enabler of subsequent technological revolution , will transform how we view, interact and use the present physical systems available around us.

It have already got major impacts on health care, smart-homes, manufacturing, commerce, education and lots of other key areas of the lifestyle . The IoT market is undergoing incredible growth and therefore the IoT industry is projected to grow tenfold by 2025. With smart cities during a foreseeable sight having automated IoT in various forms, like Unmanned Aerial Vehicles (UAVs), smart-homes, e-health devices, and contextaware Augmented Reality (AR) and computer game (VR) applications utilized in daily routines, the underlying communication networks must evolve to satisfy their needs.

Communication networks must also support autonomous operations thanks to the continuously changing services, unprecedented increase in network traffic, and increasingly complex security threat landscape thanks to the amalgamation of diverse IoT devices and services. of these challenges further add into increasing the complexity of network operations.

Artificial Intelligence (AI) with its disciplines, i.e., machine learning (ML), is that the primary enabler of an autonomous and intelligently operating network. Since the groundbreaking work of Hinton et all in 2006 on a quick training method for deep neural networks, there has been a reinvigorated interest In neural networks and other ML systems networks . The appliance of ML in wireless networks has plenty of very interesting and research articles has been published. However, this is often just not the primary age of AI where it's attracted an enormous attention of research community.

During 70s and 80s, there are immense enthusiasm and Confidence in AI in cycles, followed by periods AI winters, a term coined to elucidate low interest in AI. The current era of AI has been enhanced by advanced semiconductor technologies and the advent of cloud and distributed computing.

In spite of of these technological advancements, a number of challenges still remain today so as to successfully Deploy AI-based solutions based on competition over wireless networks. rather than considering AI as an omnipotent solution, A cautious approach and careful comparison against the state art solutions is important to form the AI-based solutions applicable and successful in future communication networks.To capitalize on IoT, increase the number of affiliates diverse devices with emerging smart services, autonomous network operations leveraging AI is inevitable. For example, the conglomeration of heterogeneous IoT devices in UAVs, e-health, manufacturing, AR/VR, wearables, and smart homes through the communication technologies will It is very difficult to distinguish a defense attack legitimate traffic, and should not be practically possible or manageable without using AI. Therefore, autonomous network operations are contemplated to be possible with embedding And the use of AI concepts, technologies and methods wireless networks. To avoid repeating the definitions of the vast number of types and disciplines of AI, during this article the term AI is mentioned techniques that are wont to

i) Collect (source) data from the network environment,

ii) Computation thereon (e.g. for classification, training and testing and

iii) Produce intelligent actionable information for the network.

This might include the specified systems of supervised, unsupervised or semi-supervised learning, to call a couple of .However, using AI on wireless networks will bring its own challenges, which cannot be worth considering in other fields Like mechanical vision and robotics, but more important communication networks, specifically within the case of IoT .

For example, gathering the data for training the system incurs network overhead. Storing the data requires storage In systems and large data, large storage systems are required. Similarly, performing computation on the info to extract actionable information requires higher computing resources. If resources

are available in high-end servers in centralized cloud systems, latency critical applications are going to be challenged Communication delays, among other factors.

In decentralized systems, sharing data and training models or parameters of AI algorithms won't only require higher communication network resources, but also open security challenges.Hence, using AI in wireless networks has many challenges that aren't counted in most of the research during this direction.

Most of the state-of-the-art research articles plan to solve specific challenges using AI in wireless networks while ignoring the resulting challenges arising as a consequence. Therefore, major challenges that arise thanks to using AI in wireless networks are discussed during this article, mainly from the point of view of IoT. the most purpose of highlighting the challenges is twofold. First, to understand research attention to the restrictions of AI from the perspectives of wireless networks. for instance , wireless channels are susceptible to errors, data distribution are often non-uniform keeping in mind the possibility of unavailability of knowledge thanks to various reasons such as jamming attacks, and wireless networks can have limited capacity like bandwidth, storage and computing required for AI.

Second, to motivate further research on developing AI based solutions that are either specific to wireless networks or avoid facing situations where solving one problem creates another within the wireless network infrastructure. for instance , learning from the large data generated by IoT with the assistance of AI within the edge might yield the specified results, however, the required storage and processing could be too costly compared to its benefits. Therefore, the way to avoid pitfalls in using AI in future wireless networks, specifically within the case of IoT, is the main theme of this text .AI for Development Series ITU BDT has launched a man-made Intelligence (AI) for Development Series to assist Information technology (ICT) regulators (NRAs) steel oneself against AI, digital transformation and therefore the digital world. The Series includes an overall framework which will 5G development examining the investment set the scene with modules on: and infrastructure requirement (to support digital transformation, AI, Internet of Things (IoT), etc.); the social and economic impact of digital transformation; AI regulation for governance; AI for society and therefore the security and data protection aspects linked to IoT and AI.

The series also includes a roadmap of actions. The module on AI and IoT in Security Aspects examines the connection between AI and IoT and analyse the safety aspects linked to AI because the key component for the complete realization of IoT. It also addresses the potential roles of competent national authorities, like NRAs in ensuring that security and data protection aspects are taken into consideration or the roll-out of IoT during this regard, this report examines the relevance of AI within the current and future development of IoT and the way security should be addressed, including data protection and privacy.

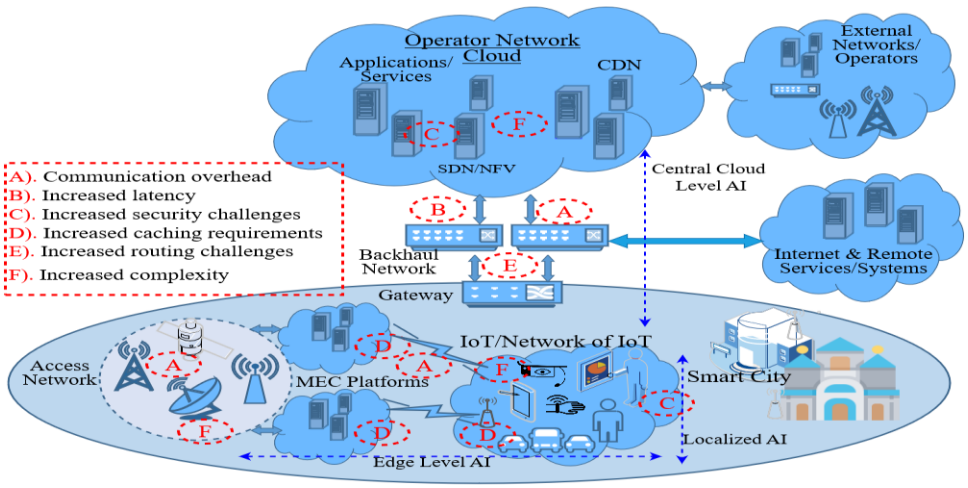
It covers the subsequent Analyse the relation between AI and IoT objectives: and the way AI is instrumental to unleash the complete Identify potential of IoT; the present landscape and threats surrounding AI-enabled IoT. What are the most challenges and therefore the commonest Provide use cases and good practices on securing IoT based applications, highlighting attack vectors?; those Analyse how standardization processes can facilitate that are AI enabled. the event of securing IoT based applications and what are the standardization requirements to make sure that AI can support such deployment.

That part will take under consideration Identify key security, privacy and trust challenges for IoT and AI the work of the ITU-T Study Group 20. also as provide indications on what solutions (policy and/or technical) are often put in situ to deal with Analyse the role of national authorities on developing regulations those challenges. that might promote safe use of IoT based applications, with specific specialise in how data processes by AI (e.g., through machine learning) are often protected, and the way privacy are often ensured.

II. CHALLENGES POSED BY AI WITHIN THE WIRELESS

NETWORK INFRASTRUCTURE

To complement for resource limitations, heterogeneity, and complexity in IoT on one hand, and large data on the opposite hand, various concepts of enhanced computing, storage, link,and bandwidth are bundled with the concepts, tools and algorithms of AI. Therefore, huge research efforts are going on during this direction . Moreover, new concepts and disciplines of AI in several network systems or network services are proposed, discussed, and evaluated continuously AI is employed in several segments, including IoT devices, and the network that connects diverse IoT devices. However, a number of challenges will surface within the when AI is employed but proper consideration isn't given to the underlying network architecture and infrastructure. during this section, we discuss the main challenges which will get on the forefront when AI is employed in future wireless networks.



A. Higher communication overhead

Using AI to enhance the efficiency of IoT devices, services offered by IoT devices, or to enhance the functionality of the underlying network employed by IoT will have additional communication overhead. The communication overhead caused by AI can be attributed to the very basic operating principles of AI systems.In IoT, the large amount of diverse data generated by the massive number of connected IoT devices would require very high memory and processing resourcesFor distributed coordinated processing of ML in multiple edge nodes, distributed ML, called federated learning, is proposed.

B. Challenges for Latency-Critical IoT Systems

The dynamic nature of future IoT services would require realtime computation, ideally near the users, or otherwise with no observable delays.However, thanks to low capacity IoT devices will take considerably longer time for AI processing within IoT devices. within the case of processing within the edge, it is concluded by Arjevani et al.Even traditional (non-ML) iterative or feedback systems are having challenges in terms of computation and link delays to satisfy the real-time requirements of dynamic services and highly mobile users.

Furthermore, the restrictions in time for usefulness of knowledge for AI processing, and validity of the result of AI mechanisms must be counted. To elaborate these limitations, consider intrusion detection systems.It took between two seconds to 5 seconds of your time when processed within the cloud. Therefore, it's concluded in that for real-time deep learning tasks, cloud isn't yet a viable solution thanks to higher latency.

C. Challenges in Routing and Network control

Although AI routing is proposed, it is traditional AI/ML techniques like artificial neural networks have evident shortcomings in terms of scalability and computation efficiency when considered for routing.A lot of research efforts are dedicated to using AI in dynamic networks. Dynamic networks have frequently changing topologies that need frequent sharing of data among nodes within the network. An example of dynamic networks is MANETs, which are composed of resource constrained mobile devices. MANETs are formed randomly and spuriously by freely moving nodes. Thus, the routing protocols usually have higher overhead thanks to dissemination of topology information, as well as sharing information due to transient disruptions during routing protocol convergence. However, the constantly changing topologies cause continuous arrival of latest information. Such systems behave sort of a closed-loop system system making it hard for the training algorithms to converge within the latency constraints. The Case of Software

Defined Networking: Since traditional network control systems heavily believe predefined policies hardwired within the data plane devices, new solutions like Software Defined Networking (SDN) have been sought to attenuate manual configurations and enable run-time changes in network policies. SDN splits the network control-data planes, centralizes the network control plane, andenables programmability of the network equipment. Thus, SDN enables dynamicity in communication networks, which is required in wireless networks to deal with sudden changes in user behavior, network traffic, and air interfaces.

Therefore, ML-based management of complex network systems, andML-based route selection in SDN, consistent with the traffic requirements of various applications are proposed and respectively. Hence, AI-based network traffic Control in STN has recently gained mainly research interest to deal with the dynamicity of mobile nodes, diverse services and increasing traffic variations.

D. Challenges in caching

Network caching systems temporarily store data or informationnear the users so as to attenuate redundant network traffic. Traditionally a router, for instance , would cache Highly demanding or frequently passed data it. However, the explosion of massive data from IoT will really challenge the basics of in-network caching. AI-based system are proposed to enable the network to find out which data or information to cache. However, using AI within the network devices, e.g. routers and switches, will consume resources meant for storing routing procedures and paths, and access control lists, etc. for instance , in the authors proposed content caching using deep learning in SDN. Considering the OpenFlow standard of SDN use In analysis, OpenPlay switches have limited support Save unsolicited flows until the controller updates the flow tables, and some sources have limited subsidiaries to save the blow rules. Furthermore, the SDN controllers have serious scalability challenges, and thus various hierarchical and distributed control plane architectures are proposed. Albeit these limitations, the authors Recommend sending a forecast output of depth. learning algorithm to the controller in order that the controller knows popularity of the contents within the network it manages. The humongous increase within the number, types and services of IoT will increase the amounts and kinds of popular content. Hence, using AI algorithms on the content within the network will require a drastic increase in memory size, also as processing capability to satisfy the wants of real-timeservices. Therefore, content caching within the edge is proposed that has its own limitations and challenges as described below.

.

III. ROADMAP: GENERALIZED GLOBAL AI ARCHITECTURE

Even though there exists a plethora of research on using AI in communication networks for various use-cases, applications, network functions and segments, little efforts are placed on visualizing the holistic specification . The major advantage of the holistic network view is to achieve the end-to-end goals without having situations where achieving one objective results in a compromise on another. additionally ,having a worldwide network view is significant to efficient utilization of available resources throughout a network. Therefore, a global network architecture using AI is presented The three tier architecture represents autonomous and intelligent network operations leveraging AI in each tier, also as across the three tiers so as to take care of synchronized AI-based operations in the entire network for various IoT services.

CONCLUSION

AI has gained a search momentum in wireless networks to deal with the increasingly complex nature of diverse IoT devices and services. However, most state-of-the-art research takes the concepts of AI from other mature technologies such as robotics and computer vision because it is and use it to solve different complex challenges faced by IoT devices and services, also because the underlying network serving IoT. Such right-away use of the concepts of AI within the wireless network infrastructure gives rise to several challenges. In this article, the most challenges are highlighted with potential solutions and open research issues that require further research. The main objective of this work is to drive attention for future research towards wireless network-specific design of the concepts, tools, algorithms, and even disciplines of AI for the communication of IoT. Furthermore, generic requirements of an IoT wireless network are highlighted to elaborate the necessity and integration points of the concepts of AI into the wireless network infrastructure employed by IoT. The challenges arising AI and wireless networks are at each integration point discussed. A generalized conceptual framework, as a roadmap, is suggested that would solve most of the challenges with novel technological concepts used for network programmability, global network resource visibility, and granular control of network and AI functions.

REFERENCES

[1] K. Ashton, “That ”Internet of Things” Thing,” RFID journal, vol. 22, no. 7, pp. 97–114, 2009.

[2] K. L. Lueth et al., “State of the IoT 2018: Number of IoT devices now at 7B–Market accelerating,” IoT Analytics, 2018.v

[3] G. E. Hinton, S. Osindero, and Y.-W. Teh, “A fast learning algorithm for deep belief nets,” Neural computation, vol. 18, no. 7, pp. 1527–1554, 2006.

[4] M. G. Kibria and K. Nguyen and G. P. Villardi and O. Zhao and K. Ishizu and F. Kojima, “Big Data Analytics, Machine Learning and Artificial Intelligence in Next-Generation Wireless Networks,” IEEE Access, vol. , no. , pp. 1–1, 2018.

[5] M. Moh and R. Raju, “Machine learning techniques for security of internet of things (IoT) and fog computing systems,” in 2018 International Conference on High Performance Computing & Simulation (HPCS). IEEE, 2018, pp. 709–715.

[6] T. Park, N. Abuzainab, and W. Saad, “Learning how to communicate in the internet of things: Finite resources and heterogeneity,” IEEE Access, vol. 4, pp. 7063–7073, 2016.