Realizing Internet of Things with Network Slicing: Opportunities and Challenges

Shalitha Wijethilaka*, Madhusanka Liyanage†
*†School of Computer Science, University College Dublin, Ireland
†Centre for Wireless Communications, University of Oulu, Finland
Email: *mahadurage.wijethilaka@ucdconnect.ie, †madhusanka@ucd.ie, †madhusanka.liyanage@oulu.fi

***Abstract*—Internet of Things (IoT) is a lucrative technology within the modern community that realizes the concept of the smart world, by expanding within a myriad of applications. Existing wireless networks require a radical change to fulfill the network requirements and cater the rapid expansion of the IoT ecosystem. 5G architecture is specifically designed to facilitate this demand. Network slicing is a pivotal technology in 5G architecture that has the ability to divide the physical network into multiple logical networks with specific network characteristics. In this paper, we are going to analyze how network slicing can be helpful in the IoT realization. Technical aspects that are required in the IoT realization, and the slicing based solutions which address these aspects, will be discussed here. Moreover, technical challenges that can arise due to network slicing integration in IoT ecosystem, will also be discussed with the potential solutions.**

***Index Terms*—5G, IoT, Network Slicing, SDN, NFV, Cloud Computing, Security, Privacy, Scalability**

I. Introduction

The evolution of the Internet has realised the concept of smart environment, connecting everything around us, to communicate with each other from anywhere, at any time. Internet of Things (IoT) is a result of this transformation and it proliferates in a plethora of applications. These applications have heterogeneous network requirements. The number of connected devices in IoT is increasing exponentially. To facilitate this rapid expansion of IoT and the diverse network requirements of its applications, architectural change in the existing telecommunication networks, is required. The novel fifth-generation (5G) architecture is specifically designed to facilitate these requirements. The variety of services provided by the 5G network are ranging over three fundamental scenarios: enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLCC), and massive Machine Type Communication (mMTC) [1]. Diversified IoT applications can be allocated into these reference scenarios.

A. What is Network Slicing

The Next Generation Network Alliance (NGMN) introduced the network slicing concept [2] to overcome the above challenges. Dividing the common physical network infrastructure to run multiple logical networks to facilitate independent business operations, is defined as the concept of network slicing [3]. Each logical network refers as a network slice, and has specific network characteristics. Software Defined Networking (SDN), Network Function Virtualization (NFV), and cloud computing are the key driving forces of the network slicing realization [4]. A network slice is composed of Network Functions (NFs) that can be physical or virtual. Network slicing can be implemented in an End-to-End (E2E) manner which spans from Radio Access Network (RAN) to core network. A fully functional network slice can route and control a packet throughout the network without getting influenced by other slices. Network slicing initiates novel business concepts such as Network Slice as a Service (NSaaS) to increase the income of Mobile Network Operators (MNOs) and to give the control of the network to third parties.

B. The role of NS in IoT

IoT has integrated into various application domains including smart transport, smart health, smart city, and home, smart grid, UAVs, industrial automation, and military operations. Each of these applications requires a set of diverse network requirements for its optimal operation. Traditional telecommunication technologies can not facilitate these requirements. Network slicing is one of the finest technologies in 5G network that can be used to fulfill these requirements. Allocating a separate slice with specific network characteristics for each IoT application over the common physical network is one of the best ways to accomplish such requirements cost-effectively. Slice isolation, dynamic deployment and rearrangement of NFs, and dynamic resource allocation between the slices are some of the possible functions that can be provided by network slicing to realize the IoT applications over 5G. Figure 1 depicts, how network slicing can be used to facilitate the diverse network requirements in different IoT applications.

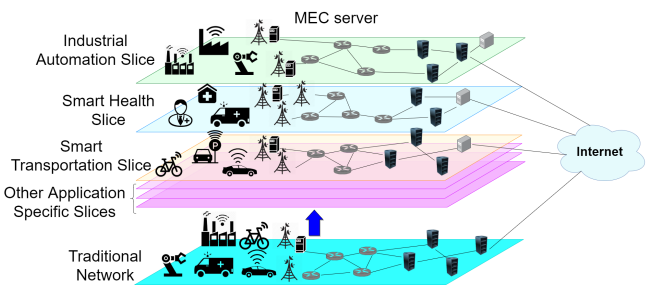

Fig. 1: Network slicing in IoT applications

C. Our Contribution and Outline of the Paper

In this paper, we address how network slicing can be utilized for the IoT realization in 5G. Section II discusses the technical benefits of using network slicing in the 5G IoT ecosystem in detail. Utilization of network slicing in the IoT ecosystem will originate some challenges such as scalability issues, frequent recursion, need of adaptive Service Function Chaining (SFC), new security and privacy issues, and complex management and orchestration. Section III discusses these challenges and the possible solutions to mitigate such challenges. Finally, section IV will conclude the paper.

II. What NS can Bring in to IoT Eco System

Network slicing can provide several technical benefits to the IoT ecosystem and this section focuses on such benefits. Why IoT requires such aspects and how network slicing facilitates these, are discussed here.

A. Improve the Scalability

IoT expands in a myriad of applications while increasing the number of connected devices exponentially. Active IoT connections which are 9.9 billion in 2020, is expected to increase more than 21 billion by 2025 [5]. This intensifies the amount of required network resources for IoT applications. Resources are scarce in telecommunication networks. Increasing the amount of resources in order to tackle this issue, is not a cost-effective solution for Service Providers (SPs). Typically, IoT devices have intermittent connectivity with the network as they are power constrained simple devices. Hence, the network resource utilization is very dynamic, and legacy static resource allocation methods may result in under-utilization or over-utilization of resources.

How NS can solve this issue : Network slicing allows allocating a dedicated slice for each application with the required network resources. Since resource utilization varies with time, idle resources can be found in some slices. Dynamically allocating such idle resources between slices as required, increases the scalability of the system. Rost et al. identified network slicing as a technology for improving flexibility and scalability in 5G networks [3]. In this way, network slicing can be used to improve the scalability as well as to increase resource utilization and reduce the infrastructure cost [6].

B. Improve the Dynamicity

In 4G-LTE based NB-IoT networks, all the IoT applications fulfill connectivity requirements through the same physical network. Moreover, pre-5G telecom networks typically have a static operational model. In a such network setting, required specific network characteristics can not be offered to each IoT application. Furthermore, the amount of available network resources remain constant for a long period for pre-5G networks due to the heavy cost of the upgrading network resources. Hence, it is not possible to dynamically upgrade/downgrade the network resources to satisfy the demands of constantly varying IoT applications. For instance, temporary fast deployment of extra network resources for an emergency or disaster situations is not possible in the conventional networks.

How NS can solve this issue : Dynamic slice allocations for the IoT applications, eliminates the static nature of the network. Separate slices with different NFs and configurations can offer the required network characteristics for the different IoT applications. Dynamic resource allocation between slices enables the efficient utilization of network resources. For instance, Jiang et al. proposed a heuristic-based admission control system to allocate resources dynamically between slices [7]. Network slicing deploys new logical networks on top of the conventional networks. It fulfills the requirement of the rapid deployment of temporary networks. Mayoral et al. experimented and showed such dynamic deployment of a temporary network over the 5G architecture by using network slicing [8].

C. Improve the Security

A majority of the IoT devices are resource constraints. Hence, strong security mechanisms are difficult to implement in the device itself. Also, device manufacturers usually pay less attention to the security aspects of their devices due to the requirement of low production costs. They usually use easily guessable credentials in IoT devices and device users are also not aware of the requirement to change such default credentials. These reasons attract more adversaries towards IoT systems and make the IoT devices more vulnerable to security attacks. Distributed Denial of Service (DDoS), zero-day, Man-In-The-Middle (MITM), ransomware, and IoT botnets, are some of the potential attacks in the IoT field [9], [10]. Since it is arduous to implement security mechanisms in the device itself, network-level solutions are required. Moreover, security requirements are different in heterogeneous IoT applications. For instance, military applications require a higher level of security than smart farming applications. Therefore, security mechanisms should be customized and implemented at different levels according to the nature of each IoT application.

How NS can solve this issue : Allocating a dedicated slice with strong slice isolation mechanisms is one of the network-level solutions to mitigate IoT security attacks. For instance, Sattar et al. proposed a mechanism to mitigate DDoS attacks using slice isolation [11]. Diverse security NFs can be deployed in the slices to achieve different levels of security in IoT applications as per their demand. NS can offer the ability to dynamically deploy security NFs and also optimize the utilization of network resources for security functions. When there is an ongoing security attack, the infected devices can be isolated into a quarantine slice until necessary actions are taken. This can reduce the impact of the attack on other services. Network slicing allows third party tenants to join in managerial tasks of their network slices. It enables them to decide how the security mechanisms should be implemented in their networks. It reduces the management overhead of MNOs and distributes the responsibility.

D. Improve the Privacy

At present, IoT devices collect and manage many different types of sensitive and personal information of people. As an

example, Medical IoTs (MIoTs) collects sensitive health information. Therefore, these data should be properly managed to protect privacy. In addition, privacy requirements are different in each IoT application as it depends on the collected data and involved stakeholders. These diverse privacy requirements can not be facilitated through traditional telecommunication networks. In some cases, IoT devices can be speared across the globe and collected information needs to be sent to a central location to conduct further processes. In such cases, the information will transport through multiple geographical boundaries which have different privacy requirements eg: General Data Protection Regulation (GDPR) in Europe. Implementing such diverse privacy requirements for different IoT tenants is a challenging task for mobile network operators.

How NS can solve this issue : Dedicated slice can be allocated to each application as a way of providing primitive privacy requirements. Strong slice isolation mechanisms and secure inter-slice communication schemes are required to preserve privacy between applications. For instance, Zhang et al. discussed a privacy-preserving communication scheme between autonomous vehicle slice and smart-grid slice [12]. NFs that are specifically designed to offer advanced privacy protection features, can be deployed in the slices to facilitate various privacy requirements in IoT applications. Dedicated and independent authentication mechanisms per slices will harden the gaining access to the entire network. Hence, this approach will increase the privacy of the communicated information within the entire network. Such a secure service-oriented authentication framework was proposed for network slicing enabled IoT services in [13].

E. Improve the QoS

QoS requirements of IoT applications are often diverse. For instance, an autonomous vehicle requires very low latency and an ultra-high level of reliability in its communications while the latency and reliability are not so critical in a smart farming application. Hence, facilitating such a diverse set of QoS requirements over a common network intensifies the need of revolutionising the design of the traditional networks [14].

How NS can solve this issue : NS can be utilized to facilitate QoS requirements via assigning a specific slice for each application with a sufficient amount of network resources. In congestion situations of a particular slice, extra network resources can be allocated to that slice from other less congested slices. Such dynamical allocations can help to mitigate performance degradation. For instance, Hoyhtya et al. used network slicing as a way of fulfilling the QoS requirements of critical applications such as communications between police officers or border guards over the public network [15].

F. Improve Resource Management

Network softwarization removes the hardware dependency to some extent in modern telecommunication networks. Most of the NFs are tend to run as software applications on top of commodity hardware. Therefore, some of the network resources can be shared between MNOs. The rapid expansion of IoT along with other 5G services increases the network resource consumption that finally becomes a challenge for MNOs to manage the network resources. Since the demand is rapidly increasing, the available network resources should be managed optimally.

How NS can solve this issue : The basic idea of network slicing is similar to the Infrastructure-as-a-Service (IaaS) in cloud computing that enables sharing of computing, storage, and networking resources [16]. Network slicing facilitates to divide network resources among different applications. Since resource utilization is not constant over time, a dynamic network slicing approach can be used to dynamically change resource allocations among the slices. A robust and efficient resource allocation framework was proposed in [17]. Zhang et al. presented a flexible resource allocation scheme between different network slices [18].

III. Technical Challenges

This section focuses on the technical challenges of integrating network slicing in IoT ecosystem. Moreover, the possible solutions for these challenges are also discussed here.

A. Scalability Issues

IoT expansion in new applications increases the number of slices in the network. Moreover, when facilitating specific network requirements such as ultra-low-latency through network slices, the service area provided by the slice becomes narrow. This increases the number of slices needed to be deployed in the network. Due to these reasons, the number of requests for the slice orchestrator is escalating. The slice management entity should be scalable to handle these requests accordingly. Moreover, slices should be scalable to handle the recurring changes in the traffic flows.

Possible Solutions : ETSI's Zero touch network & Service Management (ZSM) [49] is a potential solution that can be used to address the scalability challenges of the network slices. ZSM offers new capabilities such as self-configuration, self-monitoring, self-healing, and self-optimization, by using data-driven Artificial Intelligence/ Machine Learning (AI/ML) algorithms to further reduce human intervention. Distributed AI (DAI) [50] which is a modern approach in ML, supports to handle a large number of orchestration requests to the Network Slice Manager (NSM). Moreover, ML-based approaches proposed to increase the scalability of VNFs [51], can be extended to improve the scalability of network slices as well.

B. Frequency of Recursion

Creating larger functional blocks using multiple numbers of smaller functional blocks can be defined as the recursion. Recursion in network slicing can be identified as the creation of new network slices using existing slices while maintaining a slicing hierarchy with a parent-child relationship. However, the creation of a new slice is a relatively complex task. Since IoT use cases increase rapidly, slice creation is becoming a frequent task. Most of the time, these use cases are similar or slightly different. Thus, the required slices will also have

minimal changes. Thus, it is efficient to inherit properties from the existing slices while creating new slices. Due to this reason, recursion becomes very frequent for network slicing.

Possible Solutions : Reinforcement learning algorithms can be developed to identify the slice attributes from the existing slices with respect to the requirements in the slice creation request. Moreover, NSM is needed to be optimized for handling the recursion composition of network slices.

C. Design of Adaptive SFC

Usually, more than one network functions are required to provide a specific network service. SFC can be defined as the linkage of these network functions to form a service. To some extent, a network slice can be considered as a SFC since it is also a collection of connected NFs. Most of the NFs are VNFs in modern networks. Each VNF can be recognized as a network node and each node has a certain cost [52]. According to the changing demand, NFs require to create, scale, modify, or remove from the network to optimize the cost. Requirements such as security and privacy, of the IoT applications, are changing dynamically. This intensifies the need for changing the network functions, finally causing for modifying the SFC accordingly. Selecting the optimal nodes for the SFC and choosing the best routes between nodes are challenging issues in adaptive SFC.

Possible Solutions : ETSI's ZSM can be used as a base for addressing this challenge as well. Its abilities such as self-configuration and self-optimization and AI/ML algorithms such as deep neural networks and Long Short-Term Memory (LSTM) can be optimized to select the optimal nodes and routes for SFCs.

D. New Security Threats

Apart from the IoT related security challenges, a series of new security threats can be identified due to the network slicing exploitation. These network slicing related security issues can be divided into main three areas [53]. i.e life-cycle security for security vulnerabilities in the different phases of the network slice life cycle, inter-slice security for security breaches in between different slices, and intra-slice security for security threats in a slice itself. Proper slice isolation is one of the critical security requirements in network slicing. Since a user can connect with multiple network slices simultaneously, isolation should be implemented from the device to the core network. Third-party tenants involve in network slice management operations in addition to the MNOs via Application Programming Interfaces (APIs). These APIs can be an entry point for adversaries to perform malicious activities. In addition to these vulnerabilities, network slicing inherits series of security threats due to its enabling technologies such as SDN, NFV, and cloud computing [4].

Possible Solutions : Network slicing architecture can be extended to follow novel security-related concepts such as Security by Design (SbD) and Operational Security (OPSEC). Also, novel blockchain-based concepts can be applied for the slicing related security operations such as slice-authentication, slice brokering, and tenant-authentication. ML techniques such as neural networks, Bayesian networks, and autoencoders can be used to develop anomaly and intrusion detection schemes in the situations where API utilization by third party-tenants.

TABLE I: Role of slicing for IoT and its pertinent deployment challenges

	Advantages of using Slicing								**Integration Challenges**					
IoT Application	**Improving Scalability**	**Improving Dynamacity**	**Better E2E Service Orchestration**	**Improving Security**	**Improving Privacy**	**Improving QoS**	**Improving Resource management**		**Scalability Issues**	**Frequency of Recursion**	**Design of Adaptive SFC**	**Security Threats**	**Privacy Concerns**	**Complex Service mgt & Orc**
Smart transportation [19]–[21]	H	H	M	H	H	M	H		H	H	H	H	H	H
Industrial automation [22]–[24]	L	M	L	M	M	M	H		L	L	L	M	M	L
Smart Healthcare [25]–[27]	M	M	M	H	H	M	M		M	M	H	H	H	H
Smart home and city [28]–[31]	H	H	H	H	H	H	H		H	H	H	H	H	H
AR/VR/Gaming [32]–[34]	L	M	L	M	M	H	M		M	M	L	M	M	L
Military applications [35]–[37]	M	M	H	H	H	M	L		L	L	H	H	H	H
Smart grid [38]–[41]	L	L	M	H	H	M	M		L	L	M	H	H	M
UAVs and drones [42]–[45]	M	H	L	M	M	H	M		M	M	L	M	M	M
Farming and env. monitoring [46]–[48]	H	L	L	L	L	M	H		M	L	L	L	L	L

H High Impact M Medium Impact L Low Impact

E. New Privacy Concerns

There are new privacy concerns that will introduce by NS to IoT ecosystem. When a UE is connected to more than one network slices, adversaries get the potential to access the sensitive data of other slices. Also, inter-slice communications are required on some occasions. Then, the complete slice isolation is not possible. Moreover, the sharing of NFs and physical resources between slices can also endanger the confidentiality of the data. Finally, exposing slice related information and configurations via APIs grants intruders to impersonate as valid entities to purloin information [53].

Possible Solutions : Privacy protection concepts such as Privacy by Design (PbD) and Software Defined Privacy, can be utilized in the network slicing ecosystem to solve the above privacy concerns. Moreover, strong slice isolation mechanisms and secure inter-slice communication schemes through secure channels are required to prevent side-channel privacy leakages. In this case, tools such as zero knowledge proof of knowledge and zero knowledge argument of knowledge [54], can be utilized in inter-slice communications. Moreover, blockchain properties such as immutable, transparent, and decentralized database, along with cryptographic techniques, can be utilized to implement privacy in the network slicing ecosystem [55].

F. Complex Service Management and Orchestration

The proliferation of the number of slices in the network due to the IoT expansion in several applications and other 5G services hardens the operation of the slice management entity. Configuration changes, facilitating QoS requirements, dynamic resource allocations, and managing security and privacy requirements, of these slices, are complex. Moreover, the temporary deployment of network slices needs to be handled.

Possible Solutions : As described earlier, enabling intelligent automation by using ZSM concepts can also be a solution to mitigate this challenge. Moreover, slicing architecture can be redesigned with a new entity to handle the security and privacy-related perspectives in the slicing ecosystem as well as slicing applications. It will reduce the security management overhead on central entities. Also, new AI/ML-based algorithms can be designed to perform resource allocation and QoS management tasks automatically.

Table I summarizes the impact of the discussed technical advantages that can be achieved via network slicing, for some of the popular IoT applications. Furthermore, it depicts the severity of the impact of each technical challenge from each IoT application.

IV. Conclusion

Network slicing is a utilitarian technology in future mobile networks due to its ability to run multiple logical networks on top of a common infrastructure. IoT proliferates in a plethora of applications with diverse network requirements. Here, we showed how network slicing can be utilized to facilitate these network requirements in different IoT applications. Network slicing will help IoT realization in 5G by offering benefits such as improving scalability, dynamicity, security, privacy, QoS requirements, and resource management. However, this will leads to new implementation challenges such as scalability issues, frequency of recursion, design of adaptive SFC, new security and privacy threats, and complex management and orchestration. Some of these challenges can be resolved by using novel technological approaches such as various AI/ML techniques, blockchains, and ETSI's ZSM. However, it is still needed to design proper solutions to tackle these challenges before archiving the complete network slicing based IoT realization with 5G networks.

Acknowledgement

This work is party supported by European Union in RESPONSE 5G (Grant No: 789658) and Academy of Finland in 6Genesis (grant no. 318927) projects.

References

[1] P. C. Chih Lin I, "End to End Network Slicing," *WIRELESS WORLD RESEARCH FORUM*, 2017.

[2] N. Alliance, "Description of network slicing concept," *NGMN 5G P*, vol. 1, no. 1, 2016.

[3] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega *et al.*, "Network slicing to enable scalability and flexibility in 5g mobile networks," *IEEE Communications magazine*, vol. 55, no. 5, pp. 72–79, 2017.

[4] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[5] T. future of IoT: 10 predictions about the Internet of Things. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html

[6] M. A. Habibi, B. Han, and H. D. Schotten, "Network slicing in 5G mobile communication architecture, profit modeling, and challenges," *arXiv preprint arXiv:1707.00852*, 2017.

[7] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network slicing management & prioritization in 5G mobile systems," in *European Wireless 2016; 22th European Wireless Conference*. VDE, 2016, pp. 1–6.

[8] A. Mayoral, R. Vilalta, R. Casellas, R. Martinez, and R. Munoz, "Multi-tenant 5G network slicing architecture with dynamic deployment of virtualized tenant management and orchestration (MANO) instances," in *ECOC 2016; 42nd European Conference on Optical Communication*. VDE, 2016, pp. 1–3.

[9] N. JOSHI. (2019, may) "8 types of security threats to IoT". [Online]. Available: https://www.allerin.com/blog/8-types-of-security-threats-to-iot

[10] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys & Tutorials*, 2019.

[11] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019, pp. 82–90.

[12] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50–60, 2018.

[13] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[14] F. Z. Yousaf, M. Gramaglia, V. Friderikos, B. Gajic, D. von Hugo, B. Sayadi, V. Sciancalepore, and M. R. Crippa, "Network slicing with flexible mobility and QoS/QoE support for 5G Networks," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2017, pp. 1195–1201.

[15] M. Höyhtyä, K. Lähetkangas, J. Suomalainen, M. Hoppari, K. Kujanpää, K. T. Ngo, T. Kippola, M. Heikkilä, H. Posti, J. Mäki *et al.*, "Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control," *IEEE Access*, vol. 6, pp. 73 572–73 582, 2018.

[16] R. Su, D. Zhang, R. Venkatesan, Z. Gong, C. Li, F. Ding, F. Jiang, and Z. Zhu, "Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models," *IEEE Network*, vol. 33, no. 6, pp. 172–179, 2019.

[17] M. Leconte, G. S. Paschos, P. Mertikopoulos, and U. C. Kozat, "A resource allocation framework for network slicing," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 2177–2185.

[18] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. Aghvami, and V. C. Leung, "Network slicing based 5G and future mobile networks: mobility, resource management, and challenges," *IEEE communications magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[19] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 38–45, 2017.

[20] C. Campolo, A. Molinaro, A. Iera, R. R. Fontes, and C. E. Rothenberg, "Towards 5G network slicing for the V2X ecosystem," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 400–405.

[21] H. Khan, P. Luoto, M. Bennis, and M. Latva-aho, "On the application of network slicing for 5G-V2X," in *European Wireless 2018; 24th European Wireless Conference*. VDE, 2018, pp. 1–6.

[22] H. Wu, I. A. Tsokalo, D. Kuss, H. Salah, L. Pingel, and F. H. Fitzek, "Demonstration of network slicing for flexible conditional monitoring in industrial IoT networks," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–2.

[23] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller, and P. Popovski, "Network slicing in industry 4.0 applications: Abstraction methods and end-to-end analysis," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 12, pp. 5419–5427, 2018.

[24] V. Theodorou, K. V. Katsaros, A. Roos, E. Sakic, and V. Kulkarni, "Cross-domain network slicing for industrial applications," in *2018 European Conference on Networks and Communications (EuCNC)*. IEEE, 2018, pp. 209–213.

[25] A. Mavrogiorgou, A. Kiourtis, M. Touloupou, E. Kapassa, and D. Kyriazis, "Internet of medical things (IoMT): Acquiring and transforming data into HL7 FHIR through 5G network slicing," *Emerging Science Journal*, vol. 3, no. 2, pp. 64–77, 2019.

[26] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, F. Ippoliti, and G. M. Pérez, "Dynamic network slicing management of multimedia scenarios for future remote healthcare," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24 707–24 737, 2019.

[27] E. Kapassa, M. Touloupou, A. Mavrogiorgou, A. Kiourtis, D. Giannouli, K. Katsigianni, and D. Kyriazis, "An Innovative eHealth System Powered By 5G Network Slicing," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 2019, pp. 7–12.

[28] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in *2015 International Symposium on Consumer Electronics (ISCE)*. IEEE, 2015, pp. 1–2.

[29] E. Theodoridis, G. Mylonas, and I. Chatzigiannakis, "Developing an iot smart city framework," in *IISA 2013*. IEEE, 2013, pp. 1–6.

[30] B. Dzogovic, B. Santos, J. Noll, B. Feng, T. van Do *et al.*, "Enabling smart home with 5G network slicing," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2019, pp. 543–548.

[31] S. Chaabnia and A. Meddeb, "Slicing aware qos/qoe in software defined smart home network," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018, pp. 1–5.

[32] B. Pokric, S. Krco, D. Drajic, M. Pokric, V. Rajs, Z. Mihajlovic, P. Knezevic, and D. Jovanovic, "Augmented Reality Enabled IoT Services for Environmental Monitoring Utilising Serious Gaming Concept." *JoWUA*, vol. 6, no. 1, pp. 37–55, 2015.

[33] G. White, C. Cabrera, A. Palade, and S. Clarke, "Augmented reality in iot," in *International Conference on Service-Oriented Computing*. Springer, 2018, pp. 149–160.

[34] M. F. Alam, S. Katsikas, O. Beltramello, and S. Hadjiefthymiades, "Augmented and virtual reality based monitoring and safety system: A prototype IoT platform," *Journal of Network and Computer Applications*, vol. 89, pp. 109–119, 2017.

[35] D. E. Zheng and W. A. Carter, *Leveraging the internet of things for a more efficient and effective military*. Rowman & Littlefield, 2015.

[36] K. Wrona, "Securing the Internet of Things a military perspective," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 502–507.

[37] L. Yushi, J. Fei, and Y. Hui, "Study on application modes of military Internet of Things (MIOT)," in *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, vol. 3. IEEE, 2012, pp. 630–634.

[38] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[39] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *2010 International Conference on Advances in Energy Engineering*. IEEE, 2010, pp. 69–72.

[40] A. I. Sarwat, A. Sundararajan, and I. Parvez, "Trends and future directions of research for smart grid IoT sensor networks," in *International Symposium on Sensor Networks, Systems and Security*. Springer, 2017, pp. 45–61.

[41] L. Zhang, C. Mei, J. Li, Y. Liang, J. Song *et al.*, "A Survey on 5G Network Slicing Enabling the Smart Grid," in *2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 2019, pp. 911–916.

[42] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "UAV IoT framework views and challenges: Towards protecting drones as "Things"," *Sensors*, vol. 18, no. 11, p. 4015, 2018.

[43] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE communications surveys & tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019.

[44] C. Luo, J. Nightingale, E. Asemota, and C. Grecos, "A UAV-cloud system for disaster sensing applications," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–5.

[45] A. E. Garcia, S. Hofmann, C. Sous, L. Garcia, A. Baltaci, C. Bach, R. Wellens, D. Gera, D. Schupke, and H. E. Gonzalez, "Performance evaluation of network slicing for aerial vehicle communications," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[46] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu, and M. I. Ali, "Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 2016, pp. 442–447.

[47] J. Ruan, Y. Wang, F. T. S. Chan, X. Hu, M. Zhao, F. Zhu, B. Shi, Y. Shi, and F. Lin, "A life cycle framework of green IoT-based agriculture and its finance, operation, and management issues," *IEEE communications magazine*, vol. 57, no. 3, pp. 90–96, 2019.

[48] S. R. Shinde, A. Karode, and D. S. Suralkar, "Review on-IOT Based Environment Monitoring System," *International Journal of Electronics and Communication Engineering and Technology*, vol. 8, no. 2, 2017.

[49] ETSI. Zero touch network & service management (zsm). [Online]. Available: https://www.etsi.org/technologies/zero-touch-network-service-management

[50] F. Corea. (2019) Distributed artificial intelligence. [Online]. Available: https://medium.com/@Francesco_AI/distributed-artificial-intelligence-3e3491e0771c

[51] S. Rahman, T. Ahmed, M. Huynh, M. Tornatore, and B. Mukherjee, "Auto-scaling network resources using machine learning to improve qos and reduce cost," *arXiv preprint arXiv:1808.02975*, 2018.

[52] C. Pham, N. H. Tran, S. Ren, W. Saad, and C. S. Hong, "Traffic-aware and energy-efficient vNF placement for service chaining: Joint sampling and matching approach," *IEEE Transactions on Services Computing*, 2017.

[53] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," *IEEE Access*, 2020.

[54] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[55] Reimagining telecommunications with blockchains. [Online]. Available: http://telecoms.com/wp-content/blogs.dir/1/files/2018/05/reimagining-telecommunications-with-blockchains.pdf