Using Artificial Intelligence to Manage and Secure Computer Networks

October 11, 2020

James R. Schneider

IS 550: Information Systems Thesis/Project

Abstract

This paper describes the necessity and benefits of using artificial intelligence to manage and secure computer networks in an information system. As the requirements and infrastructure of computer networks continue to increase in complexity, traditional, centrally managed network approaches are not going to be able to efficiently administer, optimize, and secure the networks of the future. The amount of data that is being collected and saved has increased by at least one order of magnitude. Network operators that collect and save this data could leverage artificial intelligence (AI) and machine learning (ML) to allow the networks to be proactive rather than reactive, thus resulting in better performance and reliability. Some companies have already started innovating by adding virtual network assistants that are powered and driven by AI capabilities such as natural language processing. This allows for quicker troubleshooting and other insights.

AI has also been leveraged for energy-efficient routing, prediction of network disruptions, intrusion detection, and other security-related issues. However, there is still plenty of work to be done to ensure that the wireless networks of the future are efficient and secure as data transfer and communication increases between consumers and mobile devices and for the infrastructure that is going to power essential services in the community. Nevertheless, AI should not be considered a silver bullet. The proper application of AI will require human intelligence as baseline for computer network operations. All those in the AI industry should work together to ensure knowledge is shared to prevent any negative consequences of mismanaged AI.

Keywords: Artificial Intelligence, AI, Machine Learning, ML, Networks, Computer Networks, Wireless Networks, Fifth Generation, 5G, Sixth Generation 6G, Intent-based Networks

Table of Contents

Figures

Tables

Introduction

Computer networks with hundreds or thousands of devices, multiple types of devices, and various protocols are now commonplace. It is also not uncommon for virtual networks from more than one cloud provider to be connected to an on-premises network. The complexity of these types of networks can be managed by a machine better than a human. Some of the challenges that require a more intelligent and sophisticated solution include routing, load balancing, and congestion control (Singh, Arora, Saini, & Arora, 2014).

Zong, a mobile operator in Pakistan, tested its fifth generation (5G) network in August 2019 and generated download speeds greater than 1 Gbps (Technology, 2019). This type of network will allow for faster data speeds for businesses and consumers alike. Even though 5G networks have barely been deployed, more capable next-generation networks are already being researched and talked about. Machine learning (ML), a common application of artificial intelligence (AI), is expected to become a vital component of beyond 5G (B5G) networks (Wang, et al., 2020). Advancements in network technology and speed are going to make modern-day wireless networks harder for network operators to manage. Some of the operational challenges creating network complexity for mobile network operators (MNO) include the insatiable demand and increase of mobile data traffic and the dense cell deployment of 5G (Shafin et al., 2019).

5G and B5G networks are going to create new technical challenges, but these challenges can be solved in part by variations of AI. Artificial neural networks (ANN) provide the ability to predict, extract, and characterize nonlinearities from datasets that are becoming more massive every year (Yao et al., 2018). Also playing an important role is machine learning, which will be pivotal in the planning, deployment, and monitoring of 5G networks (Jkobsson, 2019). Future

management and security of wireless networks will require artificial intelligence to ensure the network remains secure and optimized.

This paper will discuss a brief history of the early stages of managing computer networks with and without artificial intelligence, followed by the evolution of wired and wireless networks and the increasing complexity of network management that has accompanied each iteration of performance and capability. Research spanning several decades will show the progress that has been made related to network configurations with and without AI; however, the focus of this paper with be on AI developments regarding network operation within the last five years and the need for AI to be combined with human intelligence and wisdom to ensure efficient operation and security of cutting-edge network infrastructure.

Problem Statement

The complexity of modern-day computer networks has surpassed a human's capacity to effectively manage and optimize them.

The daily lives of most people and businesses are affected by or depend on computer networks. In fact, the success and prevalence of applications and their features such as electronic mail, file transfers, remote log in, streaming audio and video, social network services, Internet commerce, and cloud computing has created a dependence on networking worldwide (Bezahaf et al., 2020). While there are certainly benefits related to increases in productivity, knowledge, communication, and collaboration; the Internet of Things (IoT); and cloud computing and storage, there are also downsides. One of the downsides to this dependence is what happens when there is an outage caused by hardware malfunctions, technical glitches, or even hacking: the potential

for large-scale adverse impact on economic, governmental, societal, and political activities (Bezahaf et al., 2020).

Various approaches have been used in the past to improve network performance such as adding bandwidth, prioritizing traffic, compressing data, adjusting packet sizes, changing user behavior, changing the schedule of backup processes running in the background at the wrong time, and keeping junk traffic off of the network (Withers, 2005). While these approaches can all make a difference in network performance, they do not fully address the trend of growing data usage and increasingly more complex network demands in a sustainable way.

Goal

To effectively manage and optimize computer networks, the goal is a network approach that dynamically and proactively reacts to the environment and conditions to ensure all functionality remains optimized.

Background

The Internet, one of the most used wide area networks (WANs), has evolved over time and will continue to do so. This is due in large part to the cycle of new applications, which generate new Internet traffic and behaviors, which leads to new requirements for handling the traffic, which then triggers more evolution and new designs of network architecture, which in turn promotes new applications as the cycle continues (Bezahaf et al., 2020). This cycle is illustrated in Figure 1.

Figure 1

Internet evolution cycle

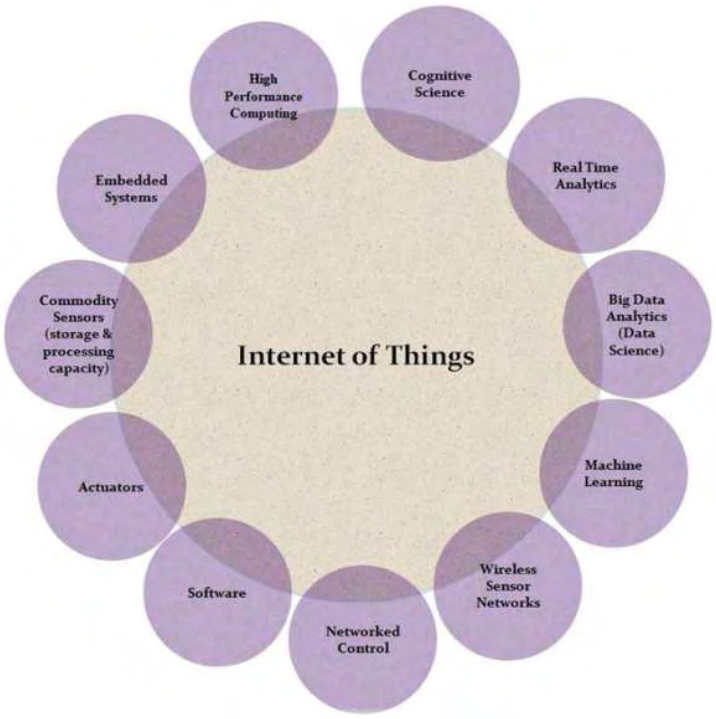
Note. Source: Bezahaf et al., 2020, p. 1.

Internet of Things

Managing modern-day computer networks includes routing, load-balancing, congestion control, and security among other things. New demands will continually be placed on networks as the number of devices connected via the Internet of things (IoT) continues to grow.

Figure 2

Fields that are merging with IoT



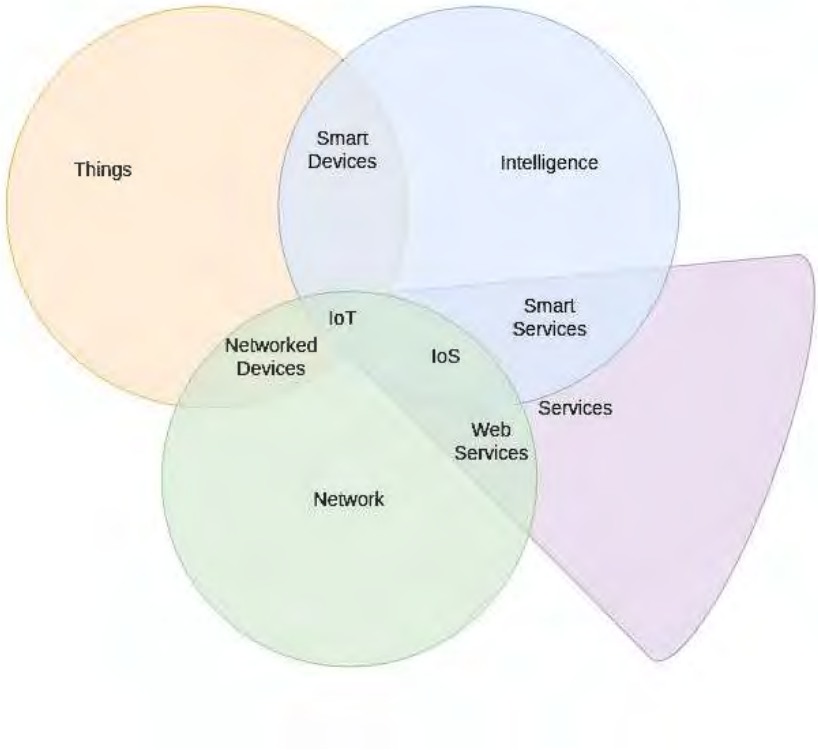
Note. Source: Ghosh et al. (2018).

The trend does not appear to be slowing down any time soon as technological capabilities are better and more economical than ever before. The Internet of everything (IoE) is a phrase being utilized as well. The IoT allows devices to communicate with each other, but the IoE describes the ability to allow everything (including living objects, non-living objects, or virtual objects) to communicate with each other (Ghosh et al. 2018). This leads to websites that can identify when a user is annoyed or excited by advertisements, offers, and other functionality because the 'things' in the physical world that make up the IoT are combined with social media,

shopping sites, and other services the comprise the Internet of services (IoS) to form the IoE (Ghosh et al. 2018).

Figure 3

Internet of Everything: Venn diagram of IoT, IoS, and IoE



Note. Source: Recreated from Ghosh et al. (2018, Fig. 2, p. 211).

AI Takes IoT to Another Level

All the data that is available by devices connected via the IoT must be processed in order to be useful. In fact, the measurement of smartness or intelligence of an IoT service depends on its level of processing (Ghosh et al., 2018). AI can help with additional processing that can lead to new insights and potential automation of tasks. Robots, voice assistants, and other smart devices

are just a few examples. But it is not just as simple as leveraging the power of AI with the IoT. What happens when the networks that the IoT depends on are not using AI?

The artificial intelligence (AI) paradigm was being considered for optimizing the topological design of distributed computer networks almost thirty years ago (Pierre, 1993), and the need to automate and secure networks due to dramatic growth in size and complexity was pointed out early on by Johnson, Derzaph & Firor (1996). However, funding and interest had begun to dissipate during that time because of previous disappointments in prior decades as AI did not live up to the optimism and hype. Nevertheless, AI has recently made a surge due to affordability and other technological advancements, resulting in it being considered as a possible and even practical solution.

AI-enabled Network Performance

As the potential benefits of artificial intelligence began to slowly pick up steam again in the early 21st century, Transmission Control Protocol (TCP) was the most extensively used protocol for the Internet (Geurtz et al., 2004). It is still one of the main protocols as of the year 2020. The benefit of machine learning for computer networks is particularly useful in wireless networks because, as Guertz et al. (2004) pointed out, TCP doesn't differentiate between network congestion and signal fading in wireless links. TCP decreases the rate of network traffic in both instances. While it may be desirable during real congestion, it is unnecessary and counterproductive when the problem is related to the wireless signal. Guertz et al. (2004) proved that three ML methods outperformed TCP congestion protocol on wireless networks.

Research by Singh et al. (2014) on the ant colony optimization (ACO) algorithm demonstrated that communication networks that employ that AI methods perform better than

non-AI modes. In every case, the average number of hops decreased. This algorithm was later combined with particle swarm optimization (PSO) to form the hybrid PSO–ACO algorithm (Heidari, 2017). The goal of this approach is optimal network reconfiguration.

Although operators have consistently tried to optimize their networks, the approach used only considers one key performance indicator (KPI) at a time (Kibria, Nguyen, Villardi, Zhao, Ishizu & Kojima, 2017). Additionally, cellular networks are currently managed based on models instead of deploying and managing networks as necessary in an ad hoc manner (Wang et al., 2020). This is troublesome because there will always be situations that occur where no models exist because the specifics have never been encountered or the environment is too nuanced to create a model.

Network capacity can't keep up with the wireless traffic load, so mobile network operators (MNO) are trying to figure out a cost-effective way to increase network capacity (Kibria et al., 2017).

AI-enabled Network Limitations

Although using AI to solve next-generation network challenges is very promising, there are some limitations and obstacles that must be overcome. Smartphones are starting to host AI agents known as on-device AI or AI at-the-edge (Yao et al., 2018). This type of technology is used in specific application contexts, which are limited in scope but likely to be implemented for physical or network layer types of problems (Yao et al., 2018). Some of the advantages to using AI at-the-edge include GPS, triangulation, connectivity (4G, 5G, Wi-Fi), and non-standard sensors such as barometers, accelerometers, and gyroscopes (Yao et al., 2018). The limitations to implementing large-scale 5G services with AI-defined functionalities include the required computational power, battery life, and memory in current-generation smartphones (Yao, et al.,

2018). One way to overcome resource deficiencies is by using AI over-the-bridge, which is applied in the cloud or base stations where resources will be in abundance (Yao et al., 2018).

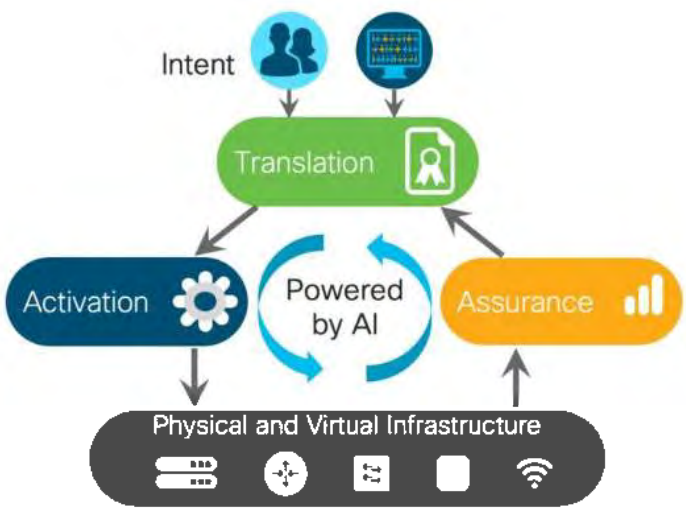
As communities begin to rely on wireless networks for integral services, privacy and security must be at the forefront of the design and implementation. AI agents could become the targets of malicious attacks, which could disrupt the network and lead to undesirable behaviors and outcomes (Yao et al., 2018).

AI-powered Network Advantages

The effects of the COVID-19 pandemic of 2020 have increased the use of video chat in schools, businesses, and government agencies in order to mitigate the risk of meeting in person. One of the features of high-quality video is low latency when viewing content and interaction via chat and video sharing. Network preparation for events like this would typically require a lot of work by humans; however, despite the human-driven efforts, it would probably not be possible to identify and fix any network problems in real time to ensure a continuous high-quality experience. (Apostolopoulos, 2019). Cisco has proposed intent-based networking (IBN) architecture as a solution that could potentially surmount this problem (Apostolopoulos, 2019). Networking can be expressed as four separate functions: Infrastructure, Assurance, Activation, and Translation (Apostolopoulos, 2019).

Figure 4

AI in intent-based networking



Note. Source: Apostolopoulos (2019).

Intent-based Networks

The following is a summary of Cisco's (2018) vision of how the four functions of an IBN could be delivered:

1. Translation – Network operators describe the desired intent for how the network should function. This could be done with a graphical user interface (GUI) or any type of predefined language or syntax. The ability to achieve this with text-to-speech expressions verbally expressed by the operators is expected to be available in the future. The Translation function then captures the intent and uses it to create a model-based policy (MBP). In order to leverage the type of automation necessary to

ensure integrity and consistency checks are applied with a sophistication beyond traditional network management, intent expressed across various network domains must be translated into standard MBPs.

2. Activation – MBPs are distributed throughout the applicable network domains with the Activation function. The orchestration function works as MBPs are disseminated into relevant domains. This allows the specific scope of network policies to be applied throughout the applicable parts of the network. Additional configuration and consistency checks can now be applied before the network elements are programmed.
3. Assurance – One of the most critical functions of intent-based networking is Assurance. Validation and verification that intent has been applied and desired outcomes have been achieved is possible after a contextual analysis of the data has been performed. There are three main aspects to Assurance:
    a) Continuous verification – Verification that system behavior is aligned with the intent expressed by network operators must occur during all stages of deployment—before, during, and after. Assurance algorithms guarantee that the state and behavior of networks are consistent with the desired intent at domain and cross-domain levels.
    b) Insights and Visibility – Analytics can provide predictions, validations, and understanding in a sophisticated manner when combined with the Assurance function. Examples include being able to predict expressed intent violations before applying changes and the ability to forecast trends.

c) Corrective actions – Anomalies and other situations that fall outside of the expressed intent can be detected and then corrected programmatically by leveraging the Activation function. These continuous optimizations are what guarantee that the expressed intent is realized automatically, or recommended adjustments can be provided to the operator.

Figure 5

Three main aspects of Assurance

Note. Source: Cisco (2018).

4. Architecture – Instead of device-by-device management, IBNs allow for networkwide system-oriented management. They also include programmable physical and virtualized infrastructure.

There are many benefits to an intent-based network approach. Cisco (2018) lists some of the most prominent ones as better compliance and security, improved business agility, reduced risk, continuous alignment between business and IT, and improved operational efficiencies. The benefits listed in Cisco's public white paper (2018) are summarized below:

Compliance and Security

Some of the main benefits of IBNs are better protection and quicker threat containment. This is achieved by including security as an integral part of each of the functional areas of an IBN. Integrity verification ensures that none of the policies in the architecture check are counteracting each other. Techniques such as advanced segmentation protect core assets by preventing the spread of infections between users and applications.

Business Agility

IBNs that are fully automated with the proper abstractions and support of application programming interfaces (API) allow new applications to be quickly integrated into a Virtual Private Cloud (VPC), an enterprise data center, or consumed as a service.

Operational Efficiency

Operational efficiency is increased, and operating expenses are reduced as network operators can reduce the time spent on testing and troubleshooting the network. The cost of network design and implementation can be reduced as well because network operators will be able to intuitively express intent which is translated into model-based policies. This model also supports the ability to scale the architecture as intent and policy are usually created at the group level. Another area that increases efficiency is the closed-loop design of IBNs. This allows the root cause of issues to quickly be determined.

Business and IT Alignment

The desired behavior of the network can be expressed abstractly in terms of what needs to be done instead of how to it. This allows the network to stay aligned with the objectives of business operations without the need of highly skilled engineers to manually translate the business objectives.

Less Risk

The error-prone processes performed via command line interfaces (CLI) are minimized. Access Control Lists (ACL) can be modified without counteracting previous policies or leaving holes in the overall security of the network. Predicting the impact of network changes can reduce the risk of an outage as well.

AI in Intent-Based Networks

The benefits of IBNs are clear, but where does AI come into play? Natural-language processing (NLP), machine learning (ML) and machine reasoning (MR) can all assist a network operator when expressing intent (Apostolopoulos, 2019). ML can also be used to predict the location of users that will be streaming data. For example, when users on an international video call will have adequate processing and bandwidth at each of their locations, or the AI can recommend that certain users find an office location (Apostolopoulos, 2019). During the call, AI will process vast amounts of real-time data to identify anything that could result in a service or security issues (Apostolopoulos, 2019). Another example of the Assurance component is the ability to reroute traffic when there is a trend showing that certain network paths are going to be saturated if action is not taken. This proactive action avoids waiting for the bottlenecks and reduction in call quality to occur (Apostolopoulos, 2019). An IBN with a feedback loop powered by AI allows the IBN and AI to amplify each other, thus resulting in actionable insights that have not been possible (Apostolopoulos, 2019). This type of solution for network congestion would helpful because Debauche et al. (2020) suggest that bottlenecks in networks are continuing to worsen because of the growing amount of data generated and quickly transported with edge computing in the cloud.

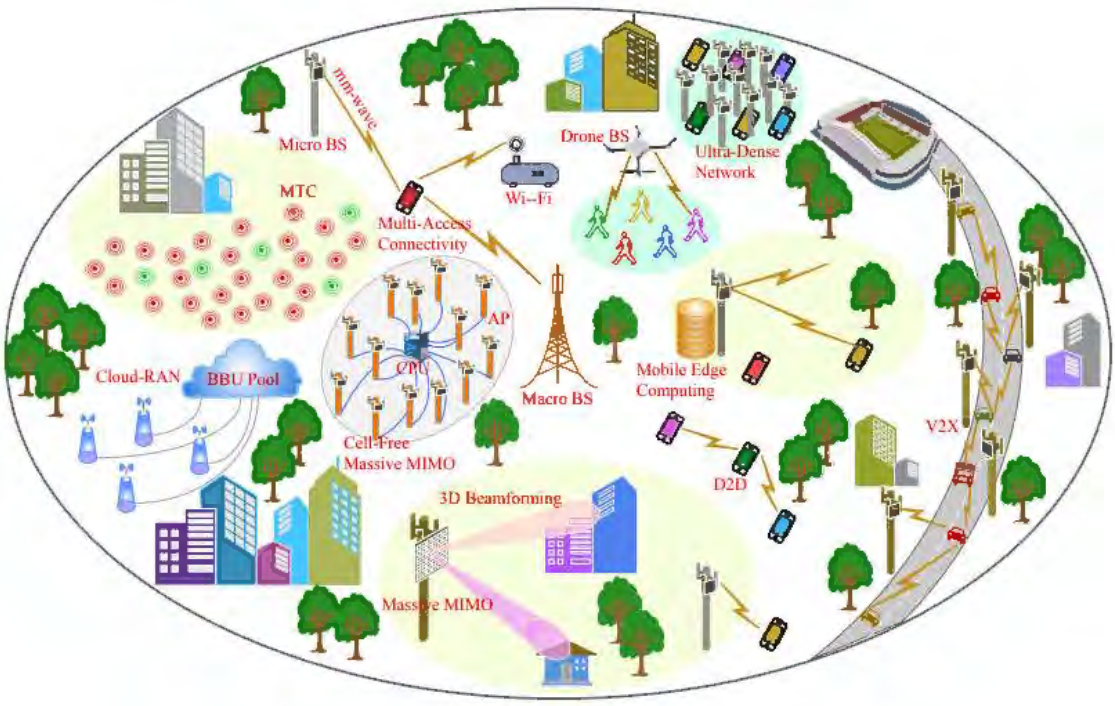
AI for Wireless Networks

For wireless networks, a solution to the new demands is to design load-distributed wireless and cellular networks that remain sturdy and well-balanced in an ever-changing and dynamic environment, which could be controlled and optimized by various types of systems, user, service, and radio analytics. AI could then use the data to make decisions that are quicker and better than humans.

Some companies are already utilizing AI within networking. Mist Systems (Mist) is using AI to ensure wireless local area networks (WLAN) are more predictable, reliable and measurable [mist.com]. One of the ways they are using AI is with natural language processing (NLP), which provides a method for the WLANs to learn. This in turn simplifies troubleshooting efforts and provides insights to the help desk and support groups (Mist, 2018).

Figure 6

Next-generation communication system



Note. Figure 2 is a next-generation communication system graphically illustrated with massive multiple-input multiple-output (MIMO), 3-dimensional (3D) beamforming, vehicle to everything (V2X), machine type communication (MTC), mobile edge computing, ultra-dense networks, and many other technological elements.

Source: Kibria et al. (2017).

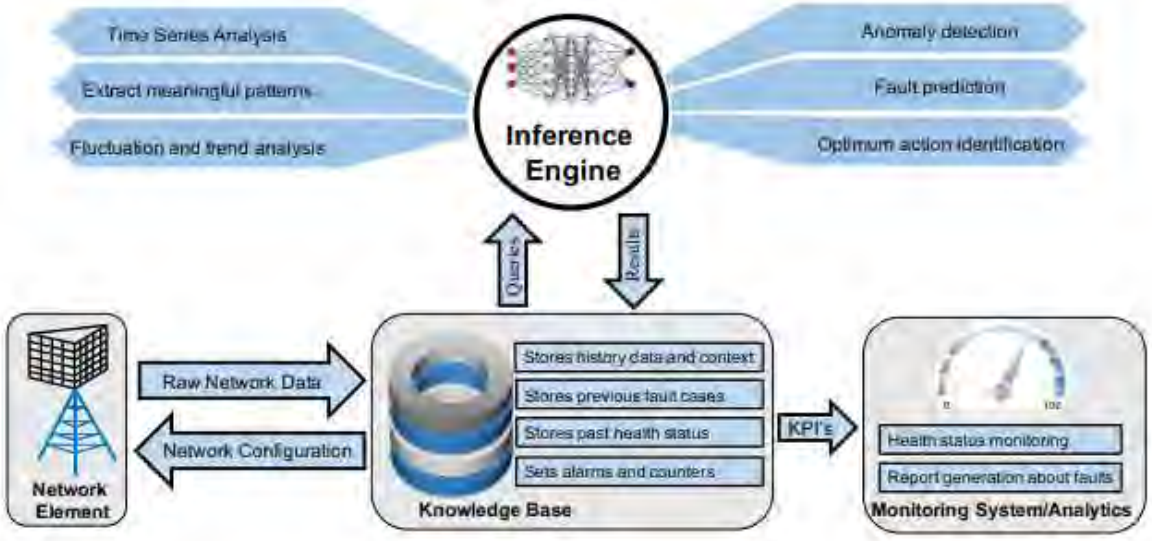
Parsing through massive datasets generated from sensor readings, drones, surveillance images, and wireless channel measurements will provide the information necessary to develop an operational map that provides a comprehensive list of devices on the network, which will support optimization efforts of functions such as user tracking and fault monitoring (Wang et al., 2020).

When compared to 4G networks, this type of radio technology uses antenna configurations that are more complex, operates and functions at higher frequencies, and utilizes beamforming as a connectivity mechanism (Jakobsson, 2019).

With the correct components in place, a self-healing network with fault detection enabled by AI is possible.

Figure 7

AI-enabled fault identification and self-healing system



Note. Source: Shafin et al., 2019.

With the type of fault recovery described in Figure 7 available, MNOs will be able to provide better service to end users, perform a root cause analysis to prevent further recurrences, and increase energy efficiency in the network. (Shafin, et al., 2019).

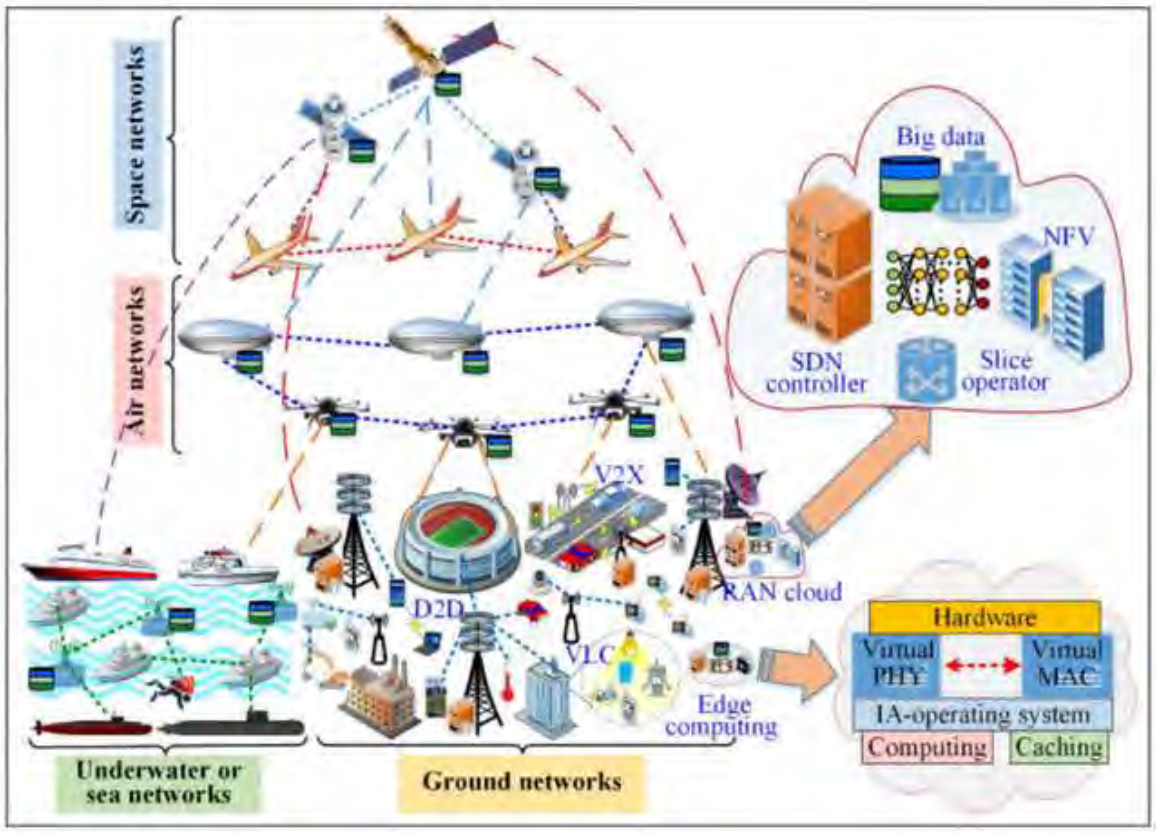
While 5G networks are being researched and deployed across the world, sixth generation (6G) networks are already being discussed as a solution for network requirements that can't be

met by 5G technology (Yang, Alphones, Xiong, Niyato, Zhao, & Wu, 2019). To support nearly instant super connectivity, integrated space-air-ground-underwater networks (ISAGUN) could make up the core architecture of future 6G networks (Yang et al., 2019). Also outlined by Yang et al. (2019) are the four tiers of ISAGUN:

1. Space-network tier: multiple satellites at different orbits are deployed to provide service to areas without ground network coverage.
2. Air-network tier: aerial platforms such as unmanned aerial vehicles (UAV), balloons, and other airships for remote areas and during urgent events.
3. Ground-network tier: principal solution for the massive number of devices that need to be supported. Bands include microwave, visible light, mmWave, Terahertz (THz), and other low-frequency bands.
4. Underwater-network tier: underwater connectivity for the communication needs of deep-sea and broad-sea activities.

Figure 8

6G network architecture



The typical architecture of 6G network (ISAGUN). V2X: vehicle to everything; VLC: visible light communication; RAN: radio access networks; SDN: software-defined networking; NFV: network function virtualization; PHY: physical layer; MAC: medium access control (Yang et al., 2019).

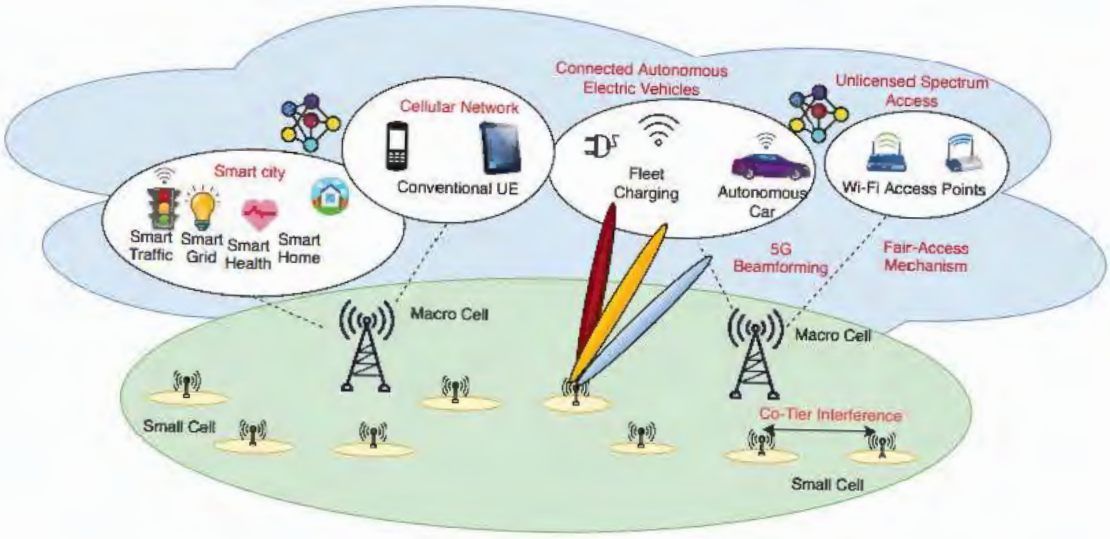
Note: The objective of ISAGUN is to [have] extremely broad coverage and seamless connectivity for space, airborne, ground, and underwater areas, such as flight in the sky, ship at sea, monitoring at remote areas or vehicles on land. As a result, human activity will dramatically expand from the ground to air, space, and deep sea. At the same time, centralized and edge computing are deployed at RAN with SND and NFV to provide powerful computational processing and massive data acquisition for ISAGUN."

Zhao et al. (2020) have documented further research related to the benefits of using AI to manage networks (summarized below):

- Supervised learning, which is when a machine learns how to map input data to an output variable based on input training data, will be used in both the physical and network layer. Channel decoding and channel states estimation can be improved in the physical layer, while traffic classification, caching, and delay mitigation can be taken care of in the network layer.
- Unsupervised learning, which only receives input data, is used to search for patterns to model the data structure without the help of output variables. Unsupervised learning can be used for traffic control and routing.
- Model-driven deep learning (DL) trains artificial neural networks (ANN) to learn from the expert information of humans to improve wireless network performance.
- Deep reinforcement learning (DRL) can be used for solving problems related to resource allocation. This will be an important problem to solve in the future as wireless networks will be required to support a wider range of users.
- Federated learning (FL) does not require a central server to host a trained model. FL could allow machine learning to be distributed across decentralized devices (edge computing) to allow for real-time learning.

Figure 9

AI-enabled 6G wireless network with related applications



Note. Source: Zhao et al., 2020, p. 5.

Mobile Edge Computing

One of the emerging technologies that will enable advanced 5G and 5GB networks is Mobile Edge Computing (MEC). MEC, a convergence of telecommunications and information technology, provides cloud computing resources at the edge of a mobile network with the objectives of reducing latency, efficient network operation, and an improved user experience (Hu et al., 2015). According to Hu et al. (2015), MEC enables the progression from 4G to 5G for several reasons:

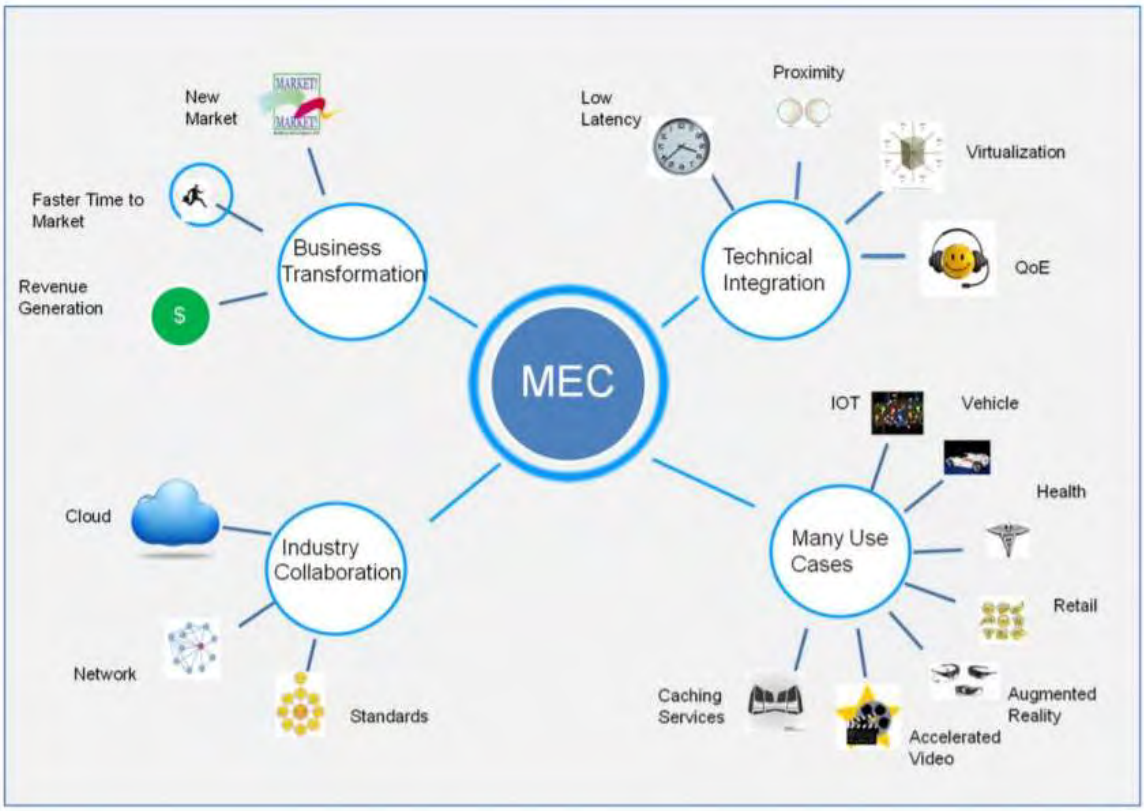
- It enables the transformation from a traditional mobile broadband network to a programmable one

- It contributes to the effort to satisfy the 5G data requirements related to automation, scalability, throughput, and latency
- Its virtualized platform is complementary to Network Functions Virtualization (NFV)
- It enables new business opportunities by giving customers the ability to use vital applications via a mobile network

Hu et al. (2015) also paint a picture of the continued growth of MEC due to market drivers such as industry collaboration, technology integration, and business transformation, all of which can be aided by MEC.

Figure 10

MEC market drivers



Note. Market drivers and use cases such as industry automation, e-Health, connected vehicles. Source: Hu et al. (2015, p. 6, Figure 1).

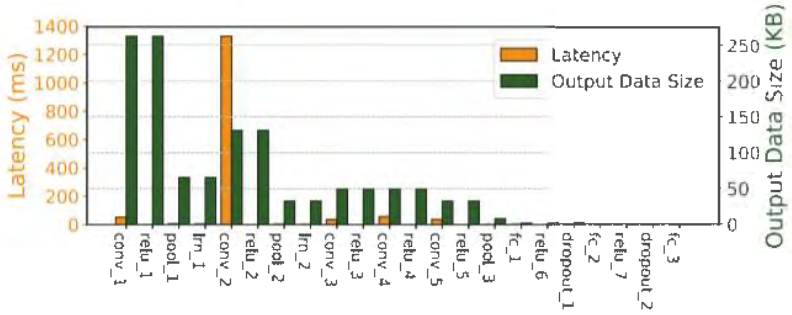
AI in Edge Computing

AI applications running on 5G networks are made possible by Deep Neural Networks (DNNs); however, the performance of tasks based on DNNs has been poor due to inadequate computation resources and network latency related to using computation resources in the cloud

(Li et al., 2019). And Li et al. (2019) also demonstrated that there is no guarantee that higher latency outputs a higher data size:

Figure 11

Runtime and output size



Note. Evidence of performance bottlenecks with DNN inference is shown above.

Source: Li et al. (2019, p.4, Figure 3).

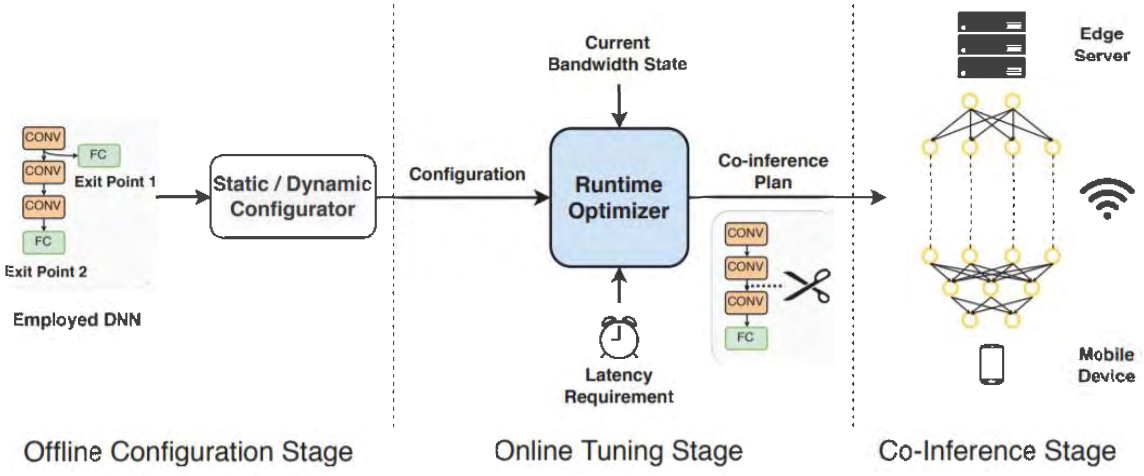
Two common strategies for solving this problem are DNN partitioning and DNN right-Sizing (Li et al., 2019). With DNN partitioning, the DNN is divided into two parts so the computation-intensive part can be offloaded at a low transmission cost while reducing latency; however, even if DNN partitioning is optimized, the computation that remains on the mobile device still creates an inference latency constraint (Li et al., 2019). DNN right-sizing can reduce the execution latency even further by using multiple branches and exit points, which would allow smaller models to have a shorter runtime (Li et al., 2019). Nevertheless, DNN right-sizing does not solve the problem without a tradeoff. Although latency is reduced in DNN right-sizing, inference accuracy is also reduced (Li et al., 2019).

Edgent is a framework that Li et al. (2019) have designed to meet latency requirements while maximizing accuracy in dynamic network conditions and bandwidth environments. This is achieved in three stages:

1. Offline configuration stage – The employed DNN is an input to a Static / Dynamic Configurator and then a configuration for online tuning is received.
2. Online tuning stage – Bandwidth is measured so DNN partitioning and DNN right-sizing can be optimized to meet latency requirements while maximizing accuracy.
3. Co-inference stage – After the exit and partition points are selected in the online tuning stage, the selected layers that precede the partition point can be executed on the edge server.

Figure 12

Edgent framework overview



Note. Source: Li et al. (2019, p. 5, Figure 5).

Network security issues

The Internet has been widely integrated into the daily lives of most people for personal and professional use. It has changed the way many people learn and has provided a new way to work. However, this also exposes people to security threats. Xin et al. (2018) focused on the importance of identifying those threats and attacks with ML, a branch of AI that is related to and overlaps with computational statistics. As discussed earlier in relation to managing wireless networks, ML can be supervised or unsupervised, is mostly based on known features learned from training data, and focuses on classification and regression. Deep learning (DL), which came after ML, attempts to simulate the human brain for analytical learning. DL can also be supervised or unsupervised. A disadvantage to DL is the requirement of more data and more high-performance

hardware. ML breaks problems into sub-problems which are solved to obtain the final while DL uses direct end-to-end problem solving. One crucial difference is interpretability. While DL performance can be amazing, the DL algorithm cannot tell you why it obtained a result, whereas ML algorithm has explicit rules. These differences must be considered when trying to solve specific network management or security-related problems.

Further research confirms that traditional computer network virus intrusion detection methods cannot meet the security requirements of the modern computer industry (Hua et al., 2019). The two main issues with traditional methods are the difficulty of operation and the fact that the whole computer cannot be evaluated, thus resulting in low evaluation accuracy (Hua et al., 2019). Potential solutions to this problem are algorithms that are part of the intrusion detection systems in a firewall. Some of the popular ones include the rule production expert system, artificial neural network, and artificial immune technology. Applying AI to computer networks can improve the firewall, anti-spam efforts, and intrusion detection (Wenhui et al. 2019).

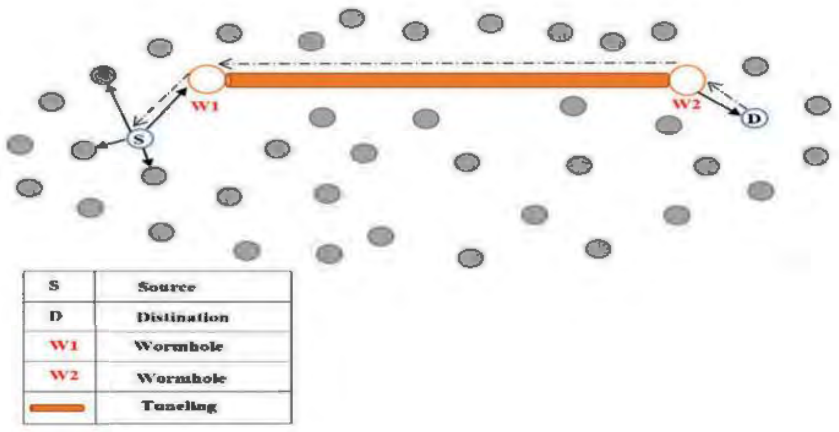
Security for Mobile Networks

A mobile ad hoc network (MANET) is a network that does not require any previous infrastructure and can be deployed spontaneously over limited geographical areas without any type of central administration (Jamali & Fotohi, 2016). One could imagine that this would be both convenient and potentially risky to have a distributed network of mobile devices without any control or defense mechanisms. One of the most common vulnerabilities in these types of networks is the wormhole attack, which is created when a malicious node finds a way to capture packets from one point in the network and then tunnels them to another point in the network

while engaging in sabotages such as data manipulation and packet dropping (Jamali & Fotohi, 2016).

Figure 13

A Mobile ad hoc network with wormhole attack



Note. Source: Jamali & Fotohi (2016, p.81, figure 1).

An artificial immune system (AIS), modeled after a human being's immune system, is what Jamali & Fotohi (2016) propose for dealing with these types of attacks. It improves performance by rapidly isolating malicious nodes without requiring complex calculations and specialized hardware (Jamali & Fotohi, 2016).

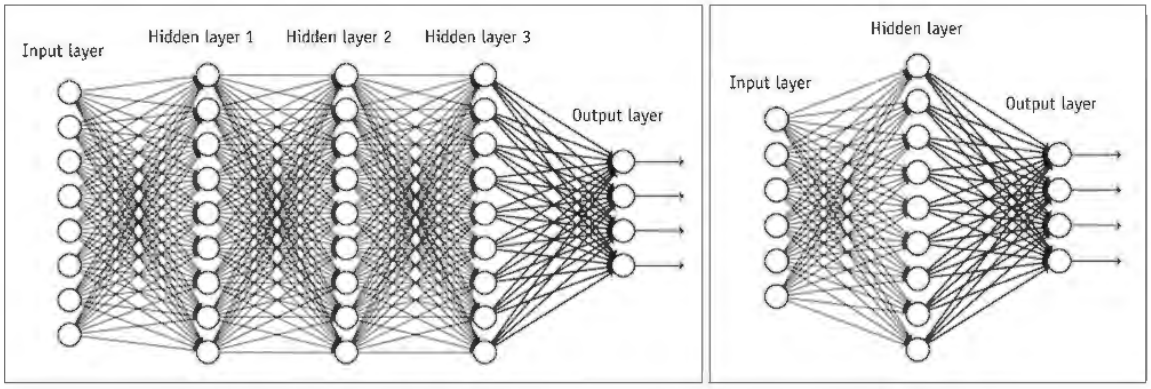
Deep and Shallow Neural Networks for Intrusion Detection

Kim & Gofman (2018) studied to efficacy of shallow and deep learning for intrusion detection. When describing neural networks, shallow and deep refer to number of layers in the

network. But adding more layers does not mean better performance—it depends on the task at hand because each can outperform the other in certain tasks. (Kim & Gofman, 2018).

Figure 14

Comparison between deep and shallow neural networks



Note. The deep neural networks used by Kim & Gofman (2018) only had two hidden layers. This picture is an example of how the layers are connected.

Source: Lee et al. (2017).

Deep neural networks tend to excel in tasks with greater complexity than shallow neural networks because some of the attributes from the lower layers can be used to learn higher level features in the top layers (Lee et al., 2017). However, in the case of network intrusion detection, shallow neural networks far outperformed deep neural networks (Kim & Gofman, 2018). The shallow neural networks had a higher accuracy and lower error rates in every experiment.

Table 1

Performance of deep and shallow neural networks on intrusion detection

Network Type	Network Performance		
	Number of Hidden Nodes	Accuracy	Error
Shallow Neural Networks	6	96.70%	3.40%
	10	97.85%	2.10%
	17	98.50%	1.40%
	20	98.45%	1.70%
Deep Neural Networks	10, 2	48.15%	53.20%
	10, 5	48.10%	52.00%
	17, 2	48.20%	51.90%
	17, 5	48.30%	51.10%
	20, 2	48.10%	51.90%
	20, 5	48.10%	52.10%

Note. Recreated from Kim & Gofman (2018, TABLE I, p. 206)

Wang et al. (2018) found that when testing network security using a neural network with one hidden layer, security management strategy had more of an impact on computer network security than routing control technology and data encryption status.

The benefits of using machine learning extends to applications and methods that depend on computer networks such as electronic mail (e-mail). The large volume of unwanted or spam e-mails prevents users from efficient user of their time, uses network bandwidth, and takes up storage capacity (Dada, et al. 2019). In addition to the irritation of spam e-mail, financial losses and security risks occur when users unwittingly click on links that are part of internet scams. Malware email-phishing scams often originate via e-mail, and then can negatively affect the networks that e-mail depends on. ML techniques that can learn and identify phishing and spam messages have been employed by leading e-mail providers (Dada et al. 2019). Google's advanced techniques can filter out spam e-mails and phishing attempts with 99.9 percent accuracy (Dada

et al. 2019). However, this is not the end of the story because spam e-mail senders will constantly look for ways to elude and evade spam filters. This is even more of a reason why ML and other AI techniques will be necessary to combat the ongoing spam and phishing attempts. Dada et al. (2019) suggest deep learning and deep adversarial learning algorithms will be able to combat the progression of spam features that allow the messages to bypass spam filters.

Risks of Artificial Intelligence

"Application of AI methods can lead to devices and systems that are untrustworthy and sometimes dangerous." (Parnas, 2017, p.30). Parnas backs up this claim with pertinent, albeit old stories and examples of the early days of AI. Problems occur when AI is misused, and rather than simulate people, machines best serve us by handling the problems that people cannot do, will not do, or do not do well (Parnas, 2017).

The Dangers of a Heuristic Approach

The issues most concerning to Parnas (2017) in terms of heuristic programming in conjunction with AI are:

1. AI does not have generally accepted definition.
2. AI programs that are almost always right and almost always work can create dependence. This could be dangerous when failures go undetected.
3. Heuristic programs, which are designed with rules of thumb in mind (experience rather than theory), are not desirable because computers execute programs without question. This contrasts with humans that can avoid instructions that will likely have negative consequences.

4. Algorithms that are verifiable are better than heuristics because devices that depend on heuristics create a facade of intelligence and additional risk.
5. AI is least risky when it would be acceptable for results to be incorrect.

Specifically pertaining to artificial neural networks (ANN), Parnas asserts that ANNs cannot do anything that conventional programs already do, and that ANNs are outperformed by conventional mathematical programs (2017). In short, ANNs are appealing but not practical (Parnas, 2017). However, it should be noted that Rojas-Delgado et al. (2019) found that using meta-heuristic algorithms reduced training time of ANNs.

Potential AI Catastrophe?

So far there have not been any significant disasters, which would likely slow down the acceptance rate of AI in any applications that could potentially have a detrimental effect on the environment or the health and safety of human beings. To ensure that the AI industry avoids any such catastrophe, competitors in the field will need to combine their resources to sustain safe and appropriate advancement (Bez & Chesbrough, 2020). If all known risks are taken on together, chances of a disaster could be reduced, problems could be more easily mitigated, and the costs for resolving the issues could be reduced (Bez & Chesbrough, 2020).

Bez & Chesbrough (2020) also suggest that the proactive approach can be put into practice with the Dynamic Capabilites Framework introduced by Teece (2007). The dynamic capabilities are sensing, seizing, and transforming:

- Sensing – promote education and training about the potential threats of the AI industry.
- Seizing – manage the way information is shared and receive commitments by creating incentives to share information.

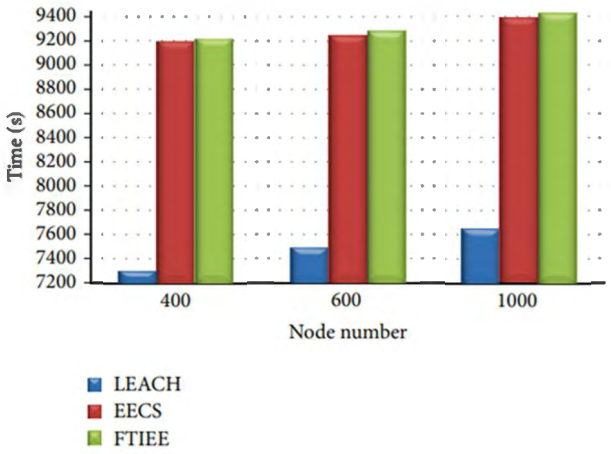
- Transforming – Implement processes which allow best practices to be used. Ensure these practices evolve rapidly when appropriate

Routing Network Traffic

Much of this paper has focused on the design, capability, and security of modern and future computer networks, but how will all the traffic be routed consistently and efficiently? Das & Tripathi (2017) proposed an optimized energy-efficient routing (OE2R) technique. The main idea behind this optimization solution is to achieve the most appropriate design relative to the specific criteria and constraints present (Das & Tripathi, 2017). By avoiding the mistake of many of the current routing techniques—focusing on one objective, Das & Tripathi can achieve this type of optimization. With the help of the combination of AI methods such as the multi-objective optimization technique (MOO) and geometric programming (GP), OE2R can lead to energy-efficient and optimized routing in hybrid ad hoc networks (HANET) (Das & Tripathi, 2017). MOO is "an optimization system where more than 1 conflicting objective functions are optimized simultaneously to get [a] single optimal solution based on multiple feasible solutions" (Das & Tripathi, 2017, p. 6, para 3). GP is "a type of mathematical optimization problem characterized by objective and constraint functions that have a special form" (Boyd et al., 2007, p. 68, para 1). It is also described as a non-linear optimization technique (Das & Tripathi, 2017). The OE2R technique has been shown to optimize the network and reduce the deterioration during communication resulting in enhanced quality of service (Das & Tripathi, 2017). Additional benefits include reduction in end-to-end delay and increased energy efficiency (Das & Tripathi, 2017).

Figure 15

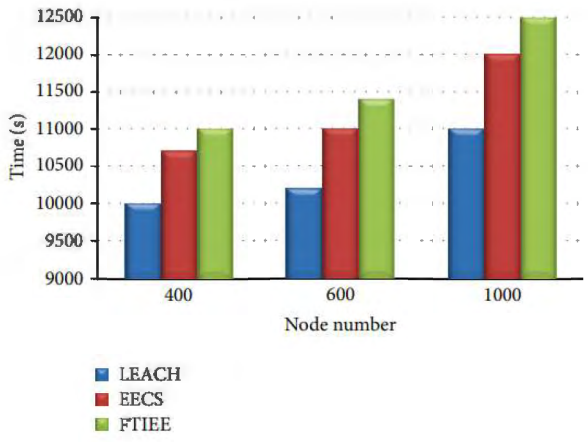
The first node time of death in LEACH, EECS, and FTIEE



Note. Source: Kiani et al. (2015, p. 10, figure 16)

Figure 16

The last node time of death in LEACH, EECS, and FTIEE



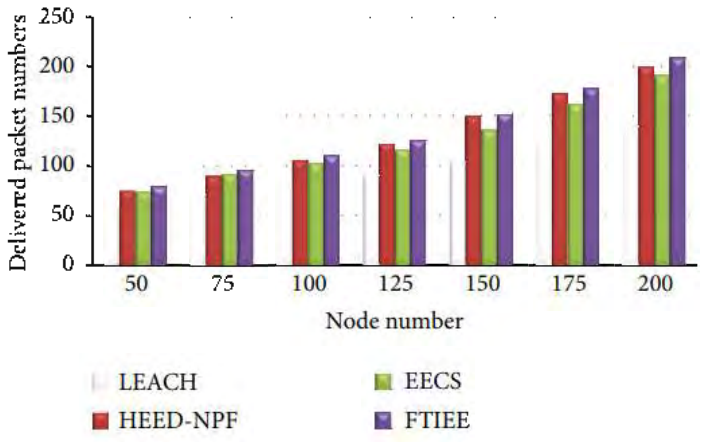
Note. Source: Kiani et al. (2015, p. 10, figure 18)

Energy-efficient Routing

The OE2R technique was not the first discovery related to energy efficiency in terms of routing. For example, the HEED (Hybrid Energy-Efficient Distributed clustering) algorithm (Younis & Fahmy, 2004) preceded the OE2R technique. Additionally, Kiana et al. (2015) designed and tested an intelligent routing protocol algorithm (FTIEE) that reduces energy consumption in individual nodes, reduces packet delays, and increases reliability and the network load balance in wireless sensor networks (WSN). Kiana et al. (2015) have improved upon the design of traditional WSN clusters. Whereas WSN clusters usually have one cluster head (CH) node, the protocol that Kiana et al. (2015) propose allows any node within a cluster to be the CH node or some clusters might not even have a CH node--the choice is made using machine learning (reinforcement learning and genetic algorithms). This is particularly helpful for reducing network overhead if a CH node were to crash. When compared with the LEACH (Heinzelman et al., 2000), HEED-NPF (Taheri et al., 2010), and EECS (Ye et al., 2005) algorithms, FTIEE outperformed them all.

Figure 17

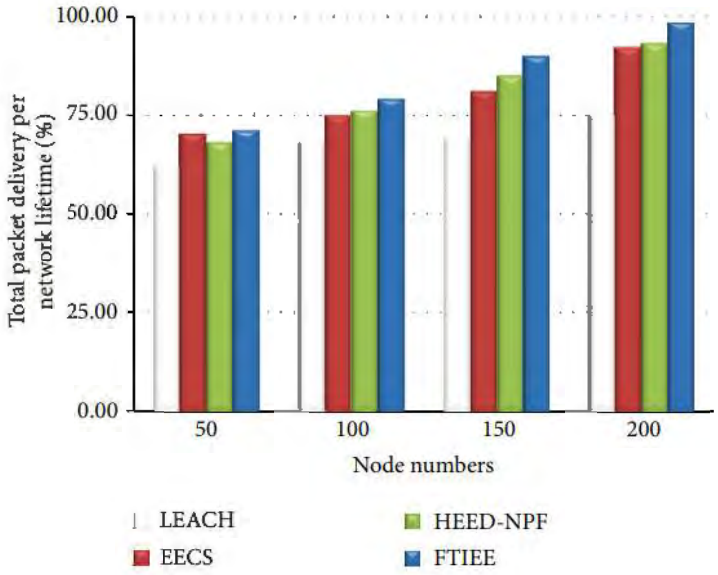
Packet delivery with different node numbers



Note. Source: Kiani et al. (2015, p. 11, figure 20)

Figure 18

Network balance performance



Note. Source: Kiani et al. (2015, p. 11, figure 21)

Proposed Solution

Finding a balanced network approach that incorporates the strengths of AI with the strengths of humans is the solution that makes the most sense. It is not a surprise that a company like Cisco, a worldwide leader in information technology, networking, and cybersecurity, is actively working on solutions that incorporates AI into an intent-based network (Cisco, 2018) that requires input from network operators before activating and assuring the network performance and architecture perform safely and efficiently according the desired intent of the network operator.

With the sheer volume of data that must be processed in 5G and beyond-5G networks, any solution that does not include some aspects of artificial intelligence will probably not be

adequate. Network bottlenecks are bound to occur—or at least the conditions that would normally cause the flow of data to be limited when thousands of devices connecting with various networks are all aiming for efficiency and productivity. Hardware and memory failures are inevitable, but with the help of AI, being able to predict those failures is not out of reach.

The author proposes that network operators choose a solution that allows human beings to decide how a network should operate at the outset, while allowing AI to make decisions within a strict purview. This would permit AI to analyze, predict, and anticipate network behavior with the goal of meeting the specified intentions of the human beings that are responsible for operating the network.

Conclusion

Computer networks are long surpassed being a nice-to-have feature of an information system. The prevalence of applications for governments, businesses, and consumers has created a dependence on networking worldwide (Bezahaf et al., 2020). The growth of the Internet of Things is not going to slow down anytime soon. By 2030, there will be an estimated 50 billion devices connected around the world (Tankovska, 2020). This certainly has the potential to lead to more network congestion. In addition to IoT, IoE describes the ability to allow everything (including living objects, non-living objects, or virtual objects) to communicate with each other (Ghosh et al. 2018). As the cycle of new applications generates new Internet traffic and behaviors, new requirements for handling the traffic will be established. This will trigger more evolution and new designs of network architecture, which in turn promotes new applications as the cycle continues (Bezahaf et al., 2020).

These are just some of the factors that must be considered when creating a sustainable plan for managing and securing the computer networks that the world depends on.

Although many efforts have been made to improve network performance such as adding bandwidth, prioritizing traffic, compressing data, adjusting packet sizes, changing user behavior, changing the schedule of backup processes running in the background at the wrong time, and keeping junk traffic off the network (Withers, 2005), the increasing complexity and interdependence of networks is going to require more than the cognitive ability of human beings in order to realize the full potential of computer networks and their various applications. To be sure, computer networks can function without the power and assistance of AI, but they will not be as efficient as they could be in terms of routing, security, and network stability. Therefore, it is worth considering AI as the next step.

The AI industry has made significant advancements during the past decade. Improvements in software and hardware have made AI more relevant than ever before. If the measurement of smartness or intelligence of an IoT service depends on its level of processing (Ghosh et al., 2018), then AI must be leveraged to crunch numbers and perform other data processing. Emerging technologies like edge computing will help make this possible, and market drivers and use cases such as industry automation, e-Health, connected vehicles (Hu et al., 2015) are going to ensure this effort continues.

AI-enabled self-healing networks will allow MNOs to provide better service to end users, perform a root cause analysis to prevent further recurrences, and increase energy efficiency in the network. (Shafin, et al., 2019).

One of the keys is knowing what AI can and cannot do. Trusting AI to be the answer to every network-related problem in an information system is not the right solution. It is only the expertise of humans that will be able to ensure that the true intent of networks is going to be achieved because "application of AI methods can lead to devices and systems that are untrustworthy and sometimes dangerous." (Parnas, 2017, p.30).

AI can be leveraged for 5G and B5G networks, edge computing, intrusion detection, energy efficient routing, and more. Even intent-based networks that have well defined activation, translation, and assurance functions can be improved with the power of AI that could process vast of amounts of data in real time that would lead to predictions of future network issues (Apostolopoulos, 2019). AI could also help network operators define the intent of the network to begin with (Apostolopoulos, 2019).

Nevertheless, humans must have the final say in how society and computer networks are managed.

Future Research

Research in the field of artificial intelligence must be a continuous process. Security has not been solved yet—nor will it ever be completely solved. Research in the area of security must evolve with the changing software, hardware, and infrastructure. Otherwise, the potential for large-scale adverse impact on economic, governmental, societal, and political activities will be a looming threat (Bezahaf et al., 2020). The bad actors are not going to rest. However, the great minds in this field can stay ahead of the curve.

To ensure that the AI industry avoids a catastrophe related due to unforeseen circumstances, competitors in the field must continue to combine their resources to sustain safe

and appropriate advancement in the field (Bez & Chesbrough, 2020). If all known risks are taken on together, chances of a disaster could be reduced, problems could be more easily mitigated, and the costs for resolving the issues could be reduced (Bez & Chesbrough, 2020). Research related to how to get all competitors to work together using the sensing, seizing, and transforming framework (Teece, 2007) would also be worthwhile. Several companies in the AI field are already participating in this effort, but new organizations must be included as well.

References

Apostolopoulos, J. (2019). Improving networks with artificial intelligence. *Cisco Blogs*. https://blogs.cisco.com/networking/improving-networks-with-ai#:~:text=Artificial%20intelligence%20is%20changing%20how,it's%20a%20change%20we%20need.&text=AI%20will%20us%20make%20network,our%20networks%20at%20machine%20speed.

Bez, S. M., & Chesbrough, H. (2020). Competitor collaboration before a crisis: What the AI industry can learn. The partnership on AI can use the dynamic capabilities framework and lessons from other industries to proactively identify AI risks and create solutions. *Research Technology Management*, 63(3), 42–48. https://doi-org.milligan.idm.oclc.org/10.1080/08956308.2020.1733889

Bezahaf, M., Hutchison, D., King, D., Race, N. (2020). *Internet evolution: Critical issues*. https://eprints.lancs.ac.uk/id/eprint/144103/3/IC_2020_01_0008.R1_Bezahaf.pdf

Boyd, S., Kim, S., Vandenberghe, L., Hassibi, A. (2007). A tutorial on geometric programming. Springer Science+Business Media, LLC. DOI 10.1007/s11081-007-9001-7

Cisco. (2018). *Intent-based networking. Building the bridge between business and IT*. [White paper]. Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-intent-networking-wp-cte-en.pdf

Dada, E., Bassi, J., Chiroma, H., Abdulhamid, S., Adetunmbi, A., Ajibuwa, O. (2019). Machine learning for email spam filtering: review, approaches and open research problems. https://reader.elsevier.com/reader/sd/pii/S2405844018353404?token=F36D4C1AF6E80DC86C0D4EFFAD5890E49E623CAC840DED67B5B75B1BA93431DC90F188F83E7E82567B3CD76506B53A24

Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems*, 30(16), 1–N.PAG. https://doi-org.milligan.idm.oclc.org/10.1002/dac.3340

Debauche, O., Mahmoudi, S., Mahmoudi, S. A., Manneback, P. & Lebeau, F. (2020). A new edge architecture for AI-IoT services deployment. *ScienceDirect, Procedia Computer Science, 175*, pp. 10-19.

Geurts, P., Khayat, I., Leduc, G. (2004). A machine learning approach to improve congestion control over wireless computer networks. https://orbi.uliege.be//bitstream/2268/4043/1/PG-ICDM2004.pdf

Ghosh, A., Chakraborty, D., Law, A. (2018). Artificial intelligence in Internet of things. IET Journals. The Institution of Engineering and Technology. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8603082

Heidari, M. (2017). Optimal network reconfiguration in distribution system for loss reduction and voltage-profile improvement using hybrid algorithm of PSO and ACO. *The Institution of Engineering and Technology*, Vol. 2017, Iss. 1, pp. 2458–2461. doi: 10.1049/oap-cired.2017.1007 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8315815

Heinzelman, W., Chandrakasan, A. & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless micro sensor networks. *33rd Annual Hawaii International Conference on System Sciences.* January 2000.

Hu, Y., Patel, M., Sabella, D., Sprecher, N. & Young, V. (2015). *Mobile Edge Computing. A key technology towards 5G* [White paper]. ETSI. https://infotech.report/Resources/Whitepapers/f205849d-0109-4de3-8c47-be52f4e4fb27_etsi_wp11_mec_a_key_technology_towards_5g.pdf

Hua, T., Li, L., Guarda, T., Lopes, I., & Rocha, Á. (2019). Computer network security technology based on artificial intelligence. J*ournal of Intelligent & Fuzzy Systems*, 37(5), 6021–6028. https://doi-org.milligan.idm.oclc.org/10.3233/JIFS-179184

Jamali, S., & Fotohi, R. (2016). Defending against Wormhole Attack in MANET Using an Artificial Immune System. New Review of Information Networking, 21(2), 79–100. https://doi-org.milligan.idm.oclc.org/10.1080/13614576.2016.1247741

Jkobsson, A. (2019, March 14). The 5G future will be powered by ai: 5G networks will demand AI because they are far more complex than previous-generation networks. AI-fueled insights will deliver higher QoE and better services. *Network Computing*. Retrieved from https://www.networkcomputing.com/wireless-infrastructure/5g-future-will-be-powered-ai

Kiani, F., Amiri, E., Zamani, M., Khodadadi, T., & Abdul Manaf, A. (2015). Efficient Intelligent Energy Routing Protocol in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, 2015, 1–13. https://doi-org.milligan.idm.oclc.org/10.1155/2015/618072

Kibria, M. G., Nguyen, K., Villardi, G. P., Zhao, O., Ishizu, K., & Kojima, F. (2017). *Big data analytics, machine learning and artificial intelligence in next-generation wireless networks*. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsarx&AN=edsarx.1711.10089&site=eds-live&scope=site

Kim, D., Gofman, M. (2018). Comparison of shallow and deep neural networks for network intrusion detection. Retrieved from https://www.researchgate.net/profile/Mikhail_Gofman2/publication/323566012_Comparison_of_shallow_and_deep_neural_networks_for_network_intrusion_detection/links/5db772c192851c81801151ca/Comparison-of-shallow-and-deep-neural-networks-for-network-intrusion-detection.pdf DOI: 10.1109/CCWC.2018.8301755

Langley, D., Doorn, J., Ng, I., Stieglitz, S., Lazovik, A., Boonstra, A. (2020). The Internet of everything: Smart things and their impact on business models. Journal of Business Research. Retrieved from https://www.sciencedirect.com/science/article/pii/S014829631930801X

Lee, J., Cho, Y., Lee, H., Kim, G., Seo, J., Kim, N. (2017). Deep learning in medical imaging: General overview. *Korean Journal of Radiology. https://www.kjronline.org/DOIx.php?id=10.3348/kjr.2017.18.4.570*

Li, E., Zeng, L. & Zhou, Z. (2019). Edge AI: On-demand accelerating deep neural network inference via Edge Computing. IEEE Transactions on Wireless Communications. XX (X). DOI: 10.1109/TWC.2019.2946140

Mist. (2018, January 30). *Mist introduces the industry's first ai-driven virtual network assistant*. [Press release]. Retrieved from https://www.mist.com/news/press-releases/mist-introduces-industrys-first-ai-driven-virtual-network-assistant/

Parnas, D. L. (2017). The Real Risks of Artificial Intelligence: Incidents from the early days of AI research are instructive in the current AI environment. *Communications of the ACM*, 60(10), 27–31. https://doi-org.milligan.idm.oclc.org/10.1145/3132724

Pierre, S. (1993). Application of artificial intelligence techniques to computer network topology design. *Engineering Applications of Artificial Intelligence Volume 6, Issue 5*, October 1993, pp 465-472. Retrieved from https://doi.org/10.1016/0952-1976(93)90007-K

Rojas-Delgado, J., Trujillo-Rasúa, R., Bello, R. (2019). A continuation approach for training Artificial Neural Networks with meta-heuristics. *Pattern Recognition Letters*, 125, 373-380. https://www.sciencedirect.com/science/article/abs/pii/S0167865519301667?via%3Dihub

Shafin, R., Liu, L., Chandrasekhar, V., Chen, H., Reed, J., Jianzhong, & Zhang. (2019). *Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G*. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsarx&AN=edsarx.1907.07862&site=eds-live&scope=site

Singh, S., Arora, S., Saini, M., & Arora, I. (2014). Estimation of effect of using ACO in dynamic routing on a communication network. *International Journal of Advanced Research in Computer Science*, 5(8), 49–53. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=scf&AN=100182780&site=eds-live&scope=site

Taheri, H., Neamatollahi, P., Naghibzadeh, M. & Yaghmaee, (M.-H. 2010). Improving on HEED protocol of wireless sensor networks using non probabilistic approach and fuzzy logic (HEEDNPF). *Proceedings of the 5th International Symposiumon Telecommunications* (IST '10), pp. 193–198, Tehran, Iran, December 2010.

Tankovska, H. (2020). IoT connected devices worldwide 2030. *Statista*. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Technology. (2019). Zong achieves 1Gbps speed on its 5G network in Pakistan. (2019). *Pakistan & Gulf Economist*, (35). Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsgao&AN=edsgcl.598314982&site=eds-live&scope=site

Teece, D. J. 2007. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*. 28(13): 1319–1350. doi:10.1002/smj.640

Wang, C.-X., Di Renzo, M., Stańczak, S., Wang, S., & Larsson, E. G. (2020). *Artificial intelligence enabled wireless networking for 5G and beyond: Recent advances and future challenges*. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsarx&AN=edsarx.2001.08159&site=eds-live&scope=site

Wang, L., Yu, J., Qiao, B., Lima, S., & Rocha, Á. (2018). Intelligent evaluation of computer network security based on neural network. Journal of Intelligent & Fuzzy Systems, 35(3), 2887–2891. https://doi-org.milligan.idm.oclc.org/10.3233/JIFS-169643

Wenhui, S., Li, C., Ren, R. (2019). Artificial intelligence and its application in computer network technology. Journal of Physics: Conf. Series 1237. doi:10.1088/1742-6596/1237/2/022142

Withers, S. (2005). 10 ways to improve network performance. *ZDNet*. https://www.zdnet.com/article/10-ways-to-improve-network-performance/

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. & Wang, C. (2018). *Machine learning and deep learning methods for cybersecurity*. IEEE Access. DOI: 10.1109/ACCESS.2018.2836950

Yang, H., Alphones, A., Xiong, Z., Niyato, D., Zhao, J., & Wu, K. (2019). *Artificial intelligence-enabled intelligent 6G networks*. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsarx&AN=edsarx.1912.05744&site=eds-live&scope=site

Yao, M., Sohul, M., Marojevic, V., & Reed, J. H. (2018). Artificial intelligence-defined 5G radio access networks. Retrieved from https://search-ebscohost-com.milligan.idm.oclc.org/login.aspx?direct=true&db=edsarx&AN=edsarx.1811.08792&site=eds-live&scope=site

Ye, M., Li, C., Chen, G. & Wu, J. (2005). EECS: an energy efficient clustering scheme in wireless sensor networks. *24th IEEE International Performance, Computing, and Communications Conference* (IPCCC '05), pp. 535–540, IEEE, April 2005.

Younis, O., & Fahmy, S. (2004). HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks. IEEE Transactions on Mobile Computing, 3(4), 366–379. https://doi-org.milligan.idm.oclc.org/10.1109/TMC.2004.41