Article

A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced Cyber-security for Critical Infrastructures

Ted H. Szymanski *

Posted Date: 8 February 2024

doi: 10.20944/preprints202402.0513.v1

Keywords: Cyber-security; Deterministic; Industrial/Tactile Internet of Things (IoT); Industry 4.0; Quantum Computers; Artificial Intelligence (AI); Zero Trust Architecture (ZTA); QKD Networks; Software-Defined-Networking (SDN); FPGAs

Article

A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced Cyber-security for Critical Infrastructures

Ted Szymanski

McMaster University, Ontario, Canada; teds@mcmaster.ca

Abstract: The next-generation "Industrial Internet of Things" (IIoT) will support "Machine-to-Machine" (M2M) communications for smart Cyber-Physical-Systems and Industry 4.0, and require guaranteed cyber-security. This paper explores hardware-enforced cyber-security for critical infrastructures. It examines a Quantum-Safe "Software-Defined Deterministic IIoT" (SDD-IIoT), with a new forwarding-plane (sub-layer-3a) for deterministic M2M traffic flows. A "Software-Defined-Networking" (SDN) control-plane controls many "SDD Wide Area Networks" (SDD-WANs), realized with FPGAs. The SDN control-plane provides an "Admission-Control/Access-Control" system for network-bandwidth, using collaborating Artificial Intelligence (AI) rule-based "Zero Trust Architectures" (ZTAs). Hardware-enforced access-control eliminates all congestion, BufferBloat, and DoS/DDoS attacks in the forwarding-plane, reduces buffer-sizes by 100,000+ times, and supports ultra-reliable and uItra-low-latency communications in the SDD-WANs. The SDD-WANs can: (i) Encrypt/Authenticate M2M flows using Quantum-Safe ciphers, to withstand attacks by Quantum Computers; (ii) Implement "Guaranteed Intrusion Detection Systems" in FPGAs, to detect cyber-attacks embedded within billions of IIoT packets/second; (iii) Provide guaranteed immunity to external cyber-attacks against critical infrastructure, and exceptionally-strong immunity to internal cyber-attacks; (iv) Save $US100s of billions annually by exploiting FPGAs; and (v) Enable "Quantum Key Distribution" (QKD) Networks by providing a programmable forwarding-plane with "authenticated classical channels" and full-immunity to DoS/DDoS attacks. Extensive experimental results for an SDD-WAN over the European Union are reported.

Keywords: cyber-security; deterministic; Industrial/Tactile Internet of Things (IoT); Industry 4.0; Quantum Computers; Artificial Intelligence (AI); Zero Trust Architecture (ZTA); QKD networks; Software-Defined-Networking (SDN); FPGAs

1. Introduction

The next-generation "Industrial Internet of Things" (IIoT) will support "Machine-to-Machine" (M2M) communications, for the future smart Cyber-Physical-Systems (CPSs), Industry 4.0, and the critical infrastructure of the 21-st century. The future CPSs include Smart Cities, Smart Transportation Systems, Smart Heathcare, the Smart Power Grid, and Smart Manufacturing. These future CPSs will require complex electronic control systems that rely upon ultra-reliable and ultra-low-latency M2M communications with full immunity to cyber-attackers. "Ultra-Reliable Low-Latency-Communications" (URLLC) for 5G/6G wireless systems are described in [1–3]. Hence, the next-generation Industrial-IoT is expected to support a "Deterministic" service model, where billions of M2M traffic flows for smart CPSs receive deterministic (i.e., guaranteed) service, with proven "Quality of Service" (QoS) guarantees, with ultra-reliable and ultra-low-latency communications, and with strict immunity to external cyber-attacks.

In contrast, the existing "Consumer Internet of Things" (Consumer-IoT) has supported "Consumer-Oriented" communications for 4 decades. It supports consumer services such as electronic shopping/e-commerce (i.e., Amazon and Alibaba), the "voice over Internet-Protocol" (i.e., voice-over-IP), video-over-IP (i.e., Netflix, Amazon Prime), music-over-IP (i.e., Spotify, Apple and Amazon Music), and social networking (i.e., Facebook, LinkedIn, and TikTok). The Consumer-IoT is based upon the layer-3 "Internet Protocol" (IP), as all traffic must pass through IP. Unfortunately, IP is over 4 decades old, and only provides a "Best-Effort" (BE) service model, with no strict (i.e., mathematically-provable) QoS guarantees [4,5]. IP is subject to significant congestion and "BufferBloat" [6,7], has poor reliability/availability, and even the layer-3 routing is insecure [8,9]. IP provides no guarantees that traffic will be delivered by a given deadline, or delivered at all.

Figure 1a illustrates a Venn Diagram, with the Consumer-IoT, the Industrial-IoT, Cyber-Physical Systems and Industry 4.0. The next-generation IoT will comprise 2 branches, the Consumer-IoT focussing on consumers, and the Industrial-IoT focussing on Industrial Automation and Industry 4.0. (Figure 1a builds upon a simpler Venn diagram illustrated in [16].) Kleinrock proposed a "Narrow-Waist" model for the protocol stack of the Consumer-IoT three decades ago in 1994. Figure 1b illustrates an evolution of the IoT protocol stack, from the "Narrow-Waist" model of the Consumer-IoT, towards a proposed "Dual Pillar" model with a "Wider-Waist", which supports both a Best-Effort pillar for the Consumer-IoT (using IP), and a Deterministic pillar for the Industrial IoT (using FPGAs and no IP).

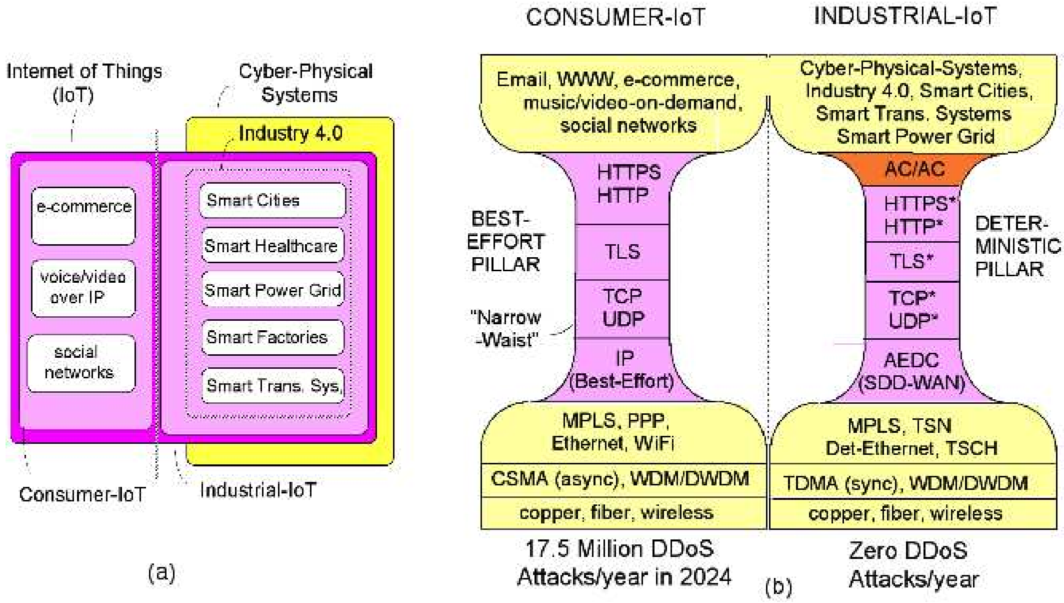


Figure 1. (a) Venn Diagram illustrating the next-generation IoT, comprising the Consumer-IoT and Industrial-IoT, Cyber-Physical-Systems and Industry 4.0. (b) A proposed "Dual Pillar" model of the next-generation IoT with a "Wider-Waist", which supports a Best-Effort pillar (using IP), and a Deterministic pillar (using FPGAs and no IP). The Deterministic pillar also includes an AI-based "Admission-Control/Access-Control" (AC/AC) system to control access to network bandwidth.

The Consumer-IoT is also vulnerable to numerous layer-3 cyber-attacks. According to Cisco, the Consumer-IoT will suffer from ≈ 17.5 million "Distributed Denial of Service" (DDoS) attacks in 2024, which can disrupt all layer-3 services [10,11]. At a growth rate of 14%, the Consumer-IoT will suffer from ≈ 20 million DDoS attacks in 2025. According to the cyber-security firm Norton, a DDoS attack is one of the "most powerful weapons on the Internet". It is a cyber-attack targeting a web-server or network, that floods it with more Internet traffic than it can handle, resulting in a loss of service. Cloudflare's global IoT network spans over 300 cities in 100 countries. It serves up to 64 million HTTP requests per second at peak times, and serves about 2.3 billion Domain Name Server (DNS) queries each day. Cloudflare mitigated over 140 billion cyber-threats per day in 2023. In 2023-Q3, Cloudflare detected and mitigated 8.9 trillion HTTP DDoS attack requests. Cloudflare estimates that the average DDoS attack lasted 8 hours in 2022, rending the targeted services unavailable for significant periods of time (several seconds, minutes or hours). Kaspersky Labs estimates that ≈ 20% of DDoS attacks last for weeks.

At the annual meeting of the "World Economic Forum" in Davos, Switzerland in Jan. 2024, the bank "JPMorgan Chase" reported that it receives billions of Internet accesses per day, many of which are attempted cyber-attacks. It reported that it spends US$15 billion a year on technology, and that it employs 62,000 technologists each year, more than Google or Amazon, many to fight cyber-attacks. In 2023, Google, Amazon, Microsoft and Cloudflare suffered record-setting DDoS attacks, called "TCP Middlebox Reflection" DDoS attacks which exploited middle-boxes, with an intensity of ≈ 200 million packets per second. Industry estimates that a DDoS attack takes up to 277 days to contain, and the average cost of a data-breach is ≈ US$10 million. DDoS attacks are also used as weapons of war, as the war between Ukraine and Russia illustrates. Clearly, the world is in the midst of a rather-severe cyber-security crisis, which grows worse every year.

The solutions proposed in this paper allow each nation to significantly-strength its national security. Each nation can achieve full immunity to external cyber-attacks, guaranteed through hardware-enforced intrusion detection, and exceptionally-strong immunity to internal cyber-attacks, for critical infrastructures on the Industrial-IoT. However, consumer-oriented entities such as banks and governments can also use the Industrial-IoT, to configure their own "Deterministic Virtual Private Networks" (D-VPNs) with exceptionally-strong cyber-security. (An "external" cyber-attacker cannot access a secured machine. An "internal" cyber-attacker has managed to obtain the secret keys needed to access a secured machine.)

Six protocols form the "Narrow-Waist" of the Consumer-IoT, as all traffic must pass through these protocols [12–15]. As shown in Figure 1b, these six protocols include:

- IP (Internet-Protocol),
- TCP ("Transmission Control Protocol"),
- UDP ("User Datagram Protocol")
- TLS ("Transport Layer Security") protocol,
- HTTP ("Hypertext Transfer Protocol"),
- HTTPS (HTTP-over-TLS).

As a result of the "Narrow-Waist" model, all Consumer-IoT traffic inherits the weaknesses of IP, i.e., the lack of deterministic QoS guarantees, and the vulnerability to layer-3 cyber-attacks, especially DoS/DDoS attacks.

According to the US CISA ("Cyber-security and Infrastructure Security Agency"), there are 16 critical infrastructure sectors in the USA, some of which are shown in Table 1 [17]. According to a recent "EU-NATO Task Force on the Resilience of Critical Infrastructure", the EU shares many of these same critical infrastructures, i.e., Energy, Transport, Digital Infrastructure, and Space [18]. The ENISA ("European Union Agency for Cybersecurity") outlines several recommendations and challenges for securing Industry 4.0.

The control-systems for these distributed critical infrastructures will require a layer-3 "Wide Area Network" (WAN) with 4 key attributes:

- (1) Ultra-High Reliability/Availability, with at least 99.999% availability (with less than 1 hour of down-time in 10 years of operation);
- (2) "Ultra-Low-Latency" (ULL) communications;
- (3) Deterministic end-to-end QoS guarantees, i.e., delay and jitter guarantees; and
- (4) Guaranteed immunity to external cyber-attacks, especially layer-3 DoS/DDoS attacks.

There is currently no known layer-3 WAN network which can meet these 4 goals. The next-generation IIoT, if it can meet these 4 key attributes, will thus provide a critical infrastructure that will support much of the world's economic activity. General Electric has estimated that the next-generation IIoT will control about one-half of global economic production by year 2030, approaching $US100 trillion in economic activity.

Table 1. Some Critical Infrastructures.

Sector	Features
Chemical	100,000s of chemical facilities, developing 70,000 diverse products. Un-interrupted transportation of chemical products.
Communications	Comprising satellite, wireless and wireline systems. CRITICAL (enables all other sectors).
Critical Manufacturing	Protect nation's manufacturing base against natural disasters & cyber-attacks. Comprises metals, machinery, electrical & transportation equipment.
Dams	Control 90,000+ dams. Protect hydro-electric generating capacity. Protect 43% of population from flooding.
Defense Industry	Over 100,000 companies provide products/services to the US military. Essential to mobilize, deploy and sustain military operations.
Energy	Electricity, oil & natural gas resources, to ensure energy for the nation. CRITICAL (enables all other sectors). Over 6,400 power plants generating over 1 Terawatt of power. Numerous pipelines to distribute fuels.
Nuclear Reactor	92 active reactors generate 20% of US energy. 8 fuel facilities, producing Uranium-235 for reactors. 3+ million shipments/year of radioactive materials.
Water & Waste Water	Over 150,000 public water systems, supplying 80% of population with safe water.
QKD Networks	Quantum Key Distribution networks may distribute "perfectly-secret" keys.
Quantum Internet	The future Quantum Internet may support nearly-unconditional security and privacy, and will achieve super-computing power.

Figure 2 illustrates the critical infrastructure comprising the main transportation corridors for the EU, which includes roads and railways. These corridors will support future "Smart Transportation Systems", which may include a vast number of automated self-driving transport trucks. Cyber-attacks targeting critical infrastructures could have serious consequences. The firm McAfee has estimated that the global costs of cybercrime were ≈ $1 Trillion in 2020. The firms Cybersecurity Ventures and Statistica estimate that the global costs of cybercrime will be ≈ US$10.5 trillion and US$17.5 trillion by 2025. The existing Consumer-IoT provides little protection against the growing threat of cyber-attacks, and cannot support the next-generation of Cyber-Physical Systems and Industry 4.0.

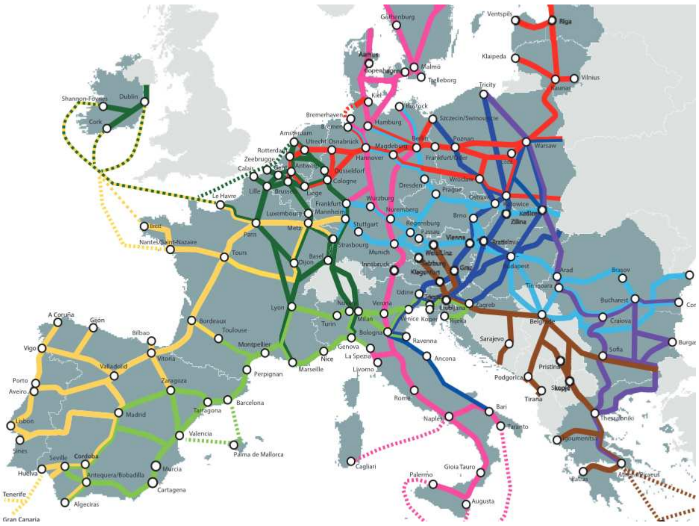


Figure 2. Map of Transportation Corridors in the European Union (critical infrastructure).

In 2008, the US "National Academy of Engineering" (NAE) identified 14 "Grand-Challenge" problems of the 21-st century. These problems include achieving: (i) clean water for the world, (ii) carbon sequestration, (iii) fusion energy, and "Security in Cyberspace" [19]. This paper explores a hardware-based approach to address the NAE grand-challenge problem of "Security in Cyber-space" for critical infrastructure. Specifically, it explores a layer-3 "Software-Defined Deterministic WAN" (SDD-WAN) architecture which can provide hardware-enforced immunity to external cyber-attacks and exceptionally-strong immunity to internal cyber-attacks, against critical infrastructure connected to the Industrial-IoT.

The proposed SDD-WANs eliminate 3 cyber-security vulnerabilities that have existed in layer-3 IP for many decades: The use of: (i) unencrypted IP packet headers; (ii) un-authenticated IP packet headers; and (iii) "middle-boxes" that implement functions such as IP address translation. The proposed SDD-WANs do not process IP packet headers, and hence they are logically-immune to all traditional IP-based cyber-attacks, in which a cyber-attacker modifies IP packet headers to perform the cyber-attack. The SDD-WANs are controlled by the SDN control-plane, not by IP packets created by cyber-attackers. The SDD-WANs enable the "Deterministic Pillar" of communications shown in Figure 1b. The Industrial-IoT replaces the IP protocol in the Best-Effort pillar, with a programmable SDD-WAN with exceptionally-strong cyber-security, in the Deterministic pillar. Hence, IP-based cyber-attacks have zero influence on the Deterministic pillar, which completely ignores IP.

As shown in Figure 1b, the Deterministic pillar can support critical infrastructure, such as the Smart Power Grid, "Quantum Key Distribution" (QKD) networks, and the future Quantum-Internet. It is well-known that critical-infrastructure such as the QKD networks (and the Quantum-Internet) require "authenticated classical channels" for control, and these channels are usually provided by dedicated point-to-point links [20]. These "authenticated classical channels" must achieve the 4 key attributes outlined earlier, including ultra-high reliability, ultra-low latency, QoS guarantees and immunity to cyber-attacks. The proposed SDD-WANs implement "Authenticated and Encrypted Deterministic Channels" (AEDCs), which can provide "authenticated classical channels" to QKD networks, in a programmable deterministic layer-3 network.

Table 2. Vulnerabilities/Problems of the Best-Effort Consumer-IoT.

Vulnerability	**Summary**
Best-Effort (BE) service model	• Provides "Best-Effort" service (no deterministic QoS guarantees). Inconsistent transmission rates, causing interference and congestion .
Access-Control or Rate-Control	• Estimated 33 billion devices in the Consumer-IoT in 2024. No "Admission-Control/Access-Control" to control transmissions. Any device can transmit to any other device, at any data-rate, at any-time, causing congestion.
Congestion and BufferBloat	• Congestion causes "BufferBloat"; Buffer-sizes given by "Bandwidth-Delay-Product" rule. 4 Tbps IP router with 1/4 sec. delay requires 1 Terabit buffer. Impossible to fit a BE-IP router with 4 Tbps capacity onto a single FPGA.
Un-encrypted and Un-authenticated IP packet headers	• IP uses unencrypted & un-authenticated packet headers. Cannot "authenticate" the sender (verify that it is who it claims to be). IoT users can modify IP packet headers to masquerade as trusted peers. Cyber-attackers can modify IP packet headers to masquerade as trusted peers.
Middle-Boxes	• Middle-Boxes perform essential functions, i.e., Address-Translation, Intrusion Detection Systems, & firewalls. Middle-boxes are insecure.
DoS and DDoS attacks	• A cyber-attacker in a compromised middle-box can generate millions of malicious IP packets causing DoS attacks. A cyber-attacker controlling many compromised IoT devices can generate millions of IP packets, causing DDoS attacks. DDoS attacks among "the most significant weapons on the Internet". • $\approx$ 17.5 million DDoS attacks in the Consumer-IoT in 2024 (Cisco). • The average DDoS attack lasted for 8 hours in 2022 (Cloudflare).
"Isolation Control"	• Cannot isolate sub-networks within the BE-IP, to contain cyber-attacks.
Over-Provisioning	• The IoT is "over-provisioned" & operates at $\leq$ 40% of peak capacity. • $\geq$60% of IoT capacity is unused (for very-high capital & energy costs).

The Narrow-Waist Model: The IP protocol in the Consumer-IoT supports a "Best-Effort" (BE) service model. It is vulnerable to congestion, BufferBloat, and layer-3 cyber-attacks, especially DoS/DDoS attacks, considered by industry as one of "the most powerful weapons on the Internet". DDoS attacks can disable a service or a sub-network for many hours, days or weeks. Hence, BE-IP traffic can be delayed by seconds, minutes, hours, days or weeks, or may never be delivered at all. DDoS attacks are discussed in [21–29].

The layer-4 TCP will guarantee that any data is delivered in the correct order. The TLS protocol will provide "cryptographic security" for end-to-end traffic flows [30]. ("Cryptographic security" can be defined as immunity to cryptographic attacks which attempt to perform eavesdropping, message tampering and message forgery [30].) However, both TCP and TLS inherit all the vulnerabilities of layer-3 IP, i.e., they rely upon the BE service of IP, and they are also vulnerable to congestion, BufferBloat, and layer-3 cyber-attacks, especially DoS/DDoS attacks. TCP and TLS flows can be delayed by seconds, minutes, hours, days or weeks, or may never be delivered at all.

As a result of congestion and BufferBloat, BE-IP routers can buffer 10s-100s of millions of packets for congested TCP and TLS flows. In the worst-case, BE-IP routers simply start "dropping" packets to relieve congestion or DoS/DDoS attacks. Hence, TLS-flows in the Consumer-IoT are effectively "unusable" for industrial control-systems.

DDoS Attacks against Servers and Networks: There are 2 types of layer-3 DoS/DDoS attacks, (i) attacks that target a web-server, and (ii) attacks that target the layer-3 network, i.e., the BE-IP routers and "Domain Name Servers" (DNSs). Cyber-attackers can easily flood a targeted web-server with millions of malicious IP packets per second, overloading the web-server and rendering the service unavailable. Web-servers using TLS-flows, with perfectly-secret keys from a QKD Network, are still vulnerable to layer-3 DoS/DDoS attacks, as the web-server is flooded with malicious traffic and unable to respond to valid traffic.

In a DoS/DDoS network attack, the attack-surface is larger than the targeted web-server, and includes every layer-3 router that supports the TLS-flow, and the DNSs in the Consumer-IoT. Each router or name-server can also be flooded with a DoS/DDoS attack, to disrupt the TLS-flow. Hence, packets in a TLS-flow suffering from a layer-3 DoS/DDoS attack can be severely delayed, or may never reach the desired web-server, rendering the TLS-flow unusable for industrial control-systems.

TLS Provides Excellent "Secrecy", but Limited "Security" against general Cyber-attacks: Table 3 illustrates several quotes on the security of the TLS protocol. The TLS protocol is perhaps the most studied Internet protocol ever, given its importance. Several quotes endorse the view that TLS provides very strong "end-to-end security" on the Internet. A few quotes question whether TLS can provide such security. Given that the world is in the midst of a deep cyber-security crisis, it is useful to determine precisely how "secure" TLS is.

According to the Internet Society, TLS provides "end-to-end security" for data sent over the Internet. According to the NIST, TLS provides a "safe communications channel" over the Internet. According to the IETF, TLS prevents "eavesdropping, forgery and message tampering" [30]. According to a 2020 ACM paper, "TLS is the defacto standard for secure communication on the Internet".

The security of TLS is established in several theoretical papers, i.e., [31–34]. These papers establish that TLS is "secure", given very specific assumptions on the types of cyber-attacks that could occur in the BE Internet. These papers typically consider Man-in-the-Middle-attacks, replay attacks, and reorder attacks. The definitions of "security" are also very specific. Reference [31] defines "security" of TLS as follows: (i) The protocol includes a secure authentication phase, and (ii) all data is transmitted using "Symmetric Key Cryptography" (SKC), to ensure confidentially. Hence, these proofs of "security" imply that the data is transmitted confidentially, and this type of security can be called "cryptographic-security". These proofs do not imply protection from any other types of cyber-attacks, other than those assumed to exist.

Table 3. Does "Transport Layer Security" (TLS) Achieve Security against all Threats?

Source	**Quotes supporting TLS Security**
Internet Society	• "TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet". Please see definition of "Security" below.
NIST	"TLS and SSL are widely used in the Internet to provide a safe communications channel for sending sensitive information".
IETF [30]	• "TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery."
IEEE [33]	• "TLS is possibly the most used protocol for secure communications, with a 18-year history of flaws and fixes".
ACM [34]	• TLS "is the defacto standard for secure communication on the internet."
Source	Quotes questioning TLS Security
NIST [40]	• "There are no known ways to prevent flooding DoS attacks against hosts visible on the Internet.
IEEE [26]	• "DDoS attacks are some of the most devastating attacks against Web applications." Application layer DoS attacks are "a major threat because of the difficulty in adopting the defenses".
firm Norton	• "A DDoS attack is one of the most powerful weapons in the Internet." It is an attack against a web-server or network that floods it with more Internet traffic than it can handle. Sophisticated cyber-criminals sell and lease software (i.e., Botnets) to create DDoS attacks on the dark web.
Dictionary	Definition of a word
Oxford	• SECURITY : "The activities involved in protecting a country, building or person against attack, danger, etc".
Oxford	• PRIVACY: "The state or condition of being free from being observed or disturbed by other people."
Oxford	• SECRECY: "The action of keeping something secret or the state of being kept secret."

It is very important to note that these theoretical proofs of TLS "cryptographic-security" [31–34] do not consider DoS/DDoS attacks, and hence they do not apply to the Consumer-IoT. DDoS attacks have been around since 1996, and the importance of DDoS attacks was highlighted in a 2004 paper [21]. Unfortunately, there are no known ways to stop these attacks.

According to NIST, "there are no known ways to prevent flooding DoS attacks against a host visible on the Internet" [40]. According to the firm Norton, DoS/DDoS attacks are one of the most "significant weapons on the Internet". According to Cisco, there will be $\approx$ 17.5 million DoS/DDoS attacks on the Consumer-Internet in 2024. Hence, the reader should note that the "TLS Security" established in theoretical papers, i.e., [31–34], implies "cryptographic security" rather than general security against all types of cyber-attacks. These theoretical papers assume that the most significant attacks on the Internet in 2024 (i.e., DoS/DDoS attacks) do not exist, and their proofs do not apply to the Consumer-IoT.

Unfortunately, the TLS protocol suffers from several vulnerabilities [35–39]. Most importantly, TLS-flows in the Consumer-IoT are vulnerable to layer-3 DoS/DDoS attacks. Even TLS-flows, using perfectly-secret keys from a QKD Network, are vulnerable to DoS/DDoS attacks. The US "National Security Agency" (NSA) acknowledges that QKD Networks are vulnerable to DoS attacks.

Given that DoS/DDoS attacks must be considered, it is clear that TLS cannot provide unconditional "end-to-end security" on the Consumer-IoT against arbitrary external cyber-attacks, as the TLS traffic might be delivered very late, or never at all. Having accurate definitions is important, given the significant costs that society incurs due to cyber-attacks.

This paper argues that TLS provides excellent "Secrecy", but limited "Security" to all types of cyber-attacks. Specifically, the TLS protocol provides excellent immunity against eavesdropping, but limited immunity to other common layer-3 external cyber-attacks, especially DoS/DDoS flooding attacks.

doi:10.20944/preprints202402.0513.v1

The Layer-3 Problems: In 2024, there is no known layer-3 network architecture which can meet the 4 key attributes stated earlier. In this paper, a "Software-Defined Deterministic Industrial Internet of Things" (SDD-IIoT) that meets these 4 goals is explored. As shown ahead in Figure 4a, a new forwarding-plane (i.e., sub-layer-3a) is introduced, to support ultra-low-latency M2M communications using "Authenticated and Encrypted Deterministic Channels" (AEDCs), also called D-flows. The forwarding-plane comprises a "Software Defined Networking" (SDN) control-plane and many authenticated SDD-WANs. Each SDD-WAN comprises many "deterministic packet switches" (D-switches), realized with "Field Programmable Gate Arrays" (FPGAs). The SDN control-plane can create millions of programmable M2M D-flows, through a network of 1,000s of authenticated D-switches, to enable the ultra-reliable and ultra-low-latency communications needed for critical infrastructure. The SDD-WANs can implement millions of programmable AEDCs in the forwarding-plane (sub-layer-3a), in FPFA hardware.

Two unique aspects of proposed SDD-IIoT will achieve exceptionally-strong hardware-enforced cyber-security: (a) The SDN control-plane implements an "Admission-Control/ Access-Control" (AC/AC) system, to control access to network bandwidth, as shown in Figure 1b. The AC/AC system comprises many "Artificial Intelligence" (AI) rule-based "Zero Trust Architectures" (ZTAs), to implement the fine-grain access-control to network bandwidth. Only M2M traffic flows that have been explicitly-approved by the AC/AC system will have reservations to communicate over the SDD-WANs in the SDD-IIoT. All other communications do not have reservations and are anomalies, i.e., malicious packets due to cyber-attacks; (b) The FPGAs will "enforce" the communications in the SDD-WANs, and will implement the "Guaranteed Intrusion Detection Systems" in hardware.

According to Cisco, the Consumer-IoT transmits about 10 billion Gigabytes of traffic per day. The FPGAs can easily process 10-100 billions of Gigabytes of IoT traffic per day, corresponding to 100s of billions of transmitted IoT packets/second, to detect and eliminate all malicious communications by external cyber-attackers, in hardware and in real-time. Hardware-based security is explored in [46–49]. Reference [47] explored hardware implementations of cryptographic functions, and identified 2 very important techniques to combat IoT vulnerabilities: (i) redundancy of hardware and (ii) redundancy of information. This paper exploits these 2 very important techniques, to achieve exceptionally-strong hardware-enforced cyber-security.

The use of an AC/AC system in the Industrial-IoT offers several benefits (some of these benefits have been established previously, and are repeated here for completeness):

- (1) It eliminates all congestion, interference, BufferBloat, and DoS/DDoS attacks [42–45];
- (2) It reduces buffer sizes in D-switches by factors of 100,000+ times, relative to a BE-IP router [42–45];
- (3) It reduces end-to-end layer-3 delays to "Ultra-Low Latencies" (ULL), i.e., the speed-of-light in fiber; [42–45];

The use of "Quantum-Safe" SDD-WANs offers several benefits:

- (4) Packets are encrypted and authenticated with Quantum-Safe ciphers, to withstand attacks by Quantum Computers [41];
- (5) Each nation can significantly-strengthen its national security. The annual number of successful "external" cyber-attacks targeting a nation's critical infrastructure can be reduced to zero[41].
- (6) The global costs of cyber-crime to society, estimated to exceed $10 trillion annually (in 2025), can be significantly reduced [41].
- (7) The global cost savings in layer-3, achieved by introducing SDN, FPGAs and determinism into layer-3, can reach US$100s of Billions per year (see section 7. This result improves upon the estimated savings of US$10s of billions presented in [41].)
- (8) The SDD-WANs can enable QKD Networks and the future Quantum Internet, by providing a programmable forwarding-plane with "authenticated classical channels" with full-immunity to external cyber-attacks (see section 5).

- (9) According to the US "National Security Agency" (NSA), QKD networks cannot authenticate the source, and are vulnerable to insider attacks and DoS attacks. The solutions typically require the use of "Pre-Shared (secret) Keys" (PSKs) and "Symmetric Key Cryptography", which lowers the security of QKD networks to the computational hardness of cracking SKC. As a result, the US NSA does not recommend QKD networks. The SDD-WANs offer comparable security to QKD networks in practice, secured by the computational hardness of cracking SKC. Hence, the SDD-WANs can provide a solution to today's cyber-security crisis, until that time when QKD networks are ready to be deployed on a large-scale to millions of users (see section 5).

An Analogy to the Aviation Industry: The goal to significantly-reduce the number of successful external cyber-attacks per year against critical-infrastructure, to zero given appropriate conditions, requires some reflection. One can ask "Is there any precedent of any other global system, which has significantly-reduced the annual number of harmful events to society to nearly zero ?". The answer is "Yes".

The global aviation system currently moves about 4 billion people per year, over many independent commercial airlines. The number of terrorists which successfully defeat the "Border Security Services" to enter the EU or USA illegally via commercial airlines is close to zero. The Border Security Services implement a basic AC/AC system: Every passenger must be (i) "authenticated" with a passport and government-issued Identification (ID), (ii) have a valid reason for travel, and (iii) must have a reservation for one seat on each flight, to track their movement and to avoid interference and congestion. The commercial airline system enforces a basic AC/AC system, using rules written on paper, enforced by humans to significantly-reduce the number of harmful events to society.

Quite remarkably, the Consumer-IoT has not used any AC/AC system for over 4 decades. The BE-IP protocol does not provide any means to authenticate the sender, and hence it cannot perform a key feature of an AC/AC system, i.e., to authenticate the users being admitted to the system. This vulnerability has existed in the Consumer-IoT for over 4 decades, and it will continue to exist for several more decades until it is addressed.

In this paper, an AC/AC system is added to the Internet, to achieve both determinism and exceptionally-strong cyber-security. This new system requires the means the authenticate the users admitted into the system, which necessitates the addition of the new Deterministic pillar, along with the new sub-layer-3a, i.e., the SDD-WAN. Artificial Intelligence (AI) is used to maintain a large "knowledge-base" of rules, potentially thousands of rules, to implement a number of "ZTAs", to yield an AC/AC system with exceptionally-strong cyber-security. FPGAs provide hardware-enforcement of the rules, and can easily process all of the global IoT traffic, to detect any and all un-authorized traffic in real-time.

Relationship to Prior Work: The links between determinism and cyber-security were first explored in 2022, i.e., an SDD-IoT and SDD-WANs and their benefits were first presented in [41]. These benefits are repeated here for completeness. Related papers on a Deterministic IoT were presented in [42–45]. Reference [41] presented some experimental results for a USA SDD-WAN. This paper focusses on Industrial Automation and the Industrial-IoT. It presents a "Dual-Pillar" model for the IoT with a "widening waist", comprising a Best-Effort pillar for the Consumer-IoT, and a Deterministic pillar for the Industrial-IoT. It presents an updated flow-chart for the SDN control-plane, which includes: (i) the IETF "Authenticated Encryption" (AE) algorithm to authenticate/encrypt M2M D-flows, and (ii) several options for key exchange, including Post-Quantum key exchange. This paper also focusses on capabilities of the hardware-enforced cyber-security, when using the latest Intel STRATIX FPGAs. It establishes that the FPGA hardware can detect cyber-attacks within 10s-100s of billions of Gigabytes of Internet traffic per day, well-above the capacity of the global Consumer-IoT in 2023. It argues that the SDD-WANs can enable QKD Networks, by providing authenticated classical channels and immunity to external cyber-attacks. It also argues that in practical deployments, the SDD-WANs have comparable cyber-security to QKD Networks (see section 5). It presents extensive experimental results for a SDD-WAN over the European-Union, operating at 100% loads using the Intel STRATIX FPGAs.

This paper is organized as follows: Section 2 briefly reviews several topics. Section 3 presents the key features of the "Deterministic IIoT". Section 4 presents the SDN control-plane. Section 5 presents the security properties. Section 6 presents experimental results for the European Union. Section 7 presents a cost analysis of layer-3. Section 8 concludes the paper. Section 9 contains the appendices; (i) a list of common acronyms, and (ii) a list of common cyber-attacks in the Consumer-IoT.

2. Review

This section reviews several topics introduced in section 1. Readers familiar with any topic can skip the review of that topic.

2.1. Problems with the Consumer-IoT

2.1.1. "Best-Effort" Service Model with No QoS Guarantees

Table 2 illustrates several vulnerabilities associated with the Consumer-IoT. The Consumer-IoT provides a "Best-Effort" service to billions of IoT devices/computers [6]. According to Cisco, in 2024 there will be about 33 billion IoT devices generating about 10 billion Gigabytes of traffic/day [10,11]. Unfortunately, the Consumer-IoT does not provide any "Admission-Control" or "Access-Control" systems to control traffic. Any IoT device is free to send IP traffic to any of the other 33 billion devices, at any data-rate and at any time. Hence, congestion and a phenomena called "BufferBloat" occur frequently [7], wherein a congested router can buffer 10s-100s of millions of packets, and end-to-end delays can be measured in seconds.

The layer-3 BGP ("Border Gateway Routing Protocol") is also insecure, vulnerable to interruptions and failures, and is expensive to fix [8,9]. Cyber-attackers can easily re-route Consumer-IoT traffic to a destination they control, by attacking the BE-IP routers. The delivery of IP packets to the correct destination is not guaranteed.

To mitigate BufferBloat, IP routers will typically start "dropping" packets from their queues when the queues become full, using a policy called "Tail Drop". A dropped packet will not be delivered to its destination, and a retransmission must be requested by the receiver, using the TCP protocol sometime in the future, adding considerable delays (typically a fraction of a second). Hence, Consumer-IoT provides a "Best-Effort" service model, with no guarantees that packets will be delivered by a deadline, or delivered at all. In practice, the Consumer-IoT functions since it is "Over-Provisioned", i.e., a significant amount of extra un-used capacity is built into the existing network, to mitigate congestion, BufferBloat and Tail-Dropping. However. this over-provisioning incurs a significant capital cost in layer-3, as shown in section 7.

2.1.2. TCP and TLS are "Best-Effort" Services

The layer-4 TCP ensures that packets are delivered to their destination in the proper order, i.e., if any packets are dropped using "Tail Dropping", a retransmission of those dropped packets is requested by the receiver sometime in the future. However, TCP inherits the vulnerabilities of the layer-3 BE-IP, i.e., (i) it relies upon a BE service model and provides no QoS guarantees, and (ii) it suffers from many layer-3 attacks, especially DoS/DDoS attacks. Hence, a congested TCP-flow can result in end-to-end delays of measured in seconds [6]. A TCP-flow suffering from a DoS/DDoS attack can incur end-to-end delays of measured in seconds, minutes, hours, days or weeks.

The TLS protocol typically resides in layers 4-7 of the Consumer-IoT. The TLS protocol will add 3 services to the data received over a TCP flow. It will ensure that: (i) the sender has been authenticated (i.e., the sender is who it claims to be), (ii) delivered traffic was encrypted when traversing layer-3, and (iii) the integrity of the data was been preserved (i.e., the message has not been altered) [30]. The TLS 1.3 protocol uses the IETF "Authenticated Encryption" (AE) algorithm, wherein each packet is encrypted with the Chacha20 stream cipher, and includes a Poly1305 "Message Authentication

Code" (MAC) to authenticate the sender, and to ensure the data integrity (i.e., the data has not been altered) [50].

However, TLS also inherits all the vulnerabilities of layer-3 IP, i.e., (i) it relies upon the Best-Effort service of IP and provides no QoS guarantees, and (ii) it suffers from many layer-3 attacks, especially DoS/DDoS attacks. Hence, a congested TLS-flow can result in end-to-end delays measured in seconds [6]. A TLS-flow suffering from a DoS/DDoS attack can incur end-to-end delays of measured in seconds, minutes, hours, days or weeks. (The "Secure Socket Layer" (SSL) protocol is the predecessor of TLS [30], and suffers from the same vulnerabilities.)

2.1.3. TLS - No Protection Against "LOG4J" Cyber-Attacks

The "LOG4J" cyber-attack discovered in 2021 has been described as "one of the most serious vulnerabilities" ever discovered by the US CISA ("Cyber-Security and Infrastructure Security") agency, and may take years to fully resolve.

Many serious cyber-attacks occur when a cyber-attacker gains control of a secured web-server (called a “Remote Code Execution” attack in the Appendix). In the “LOG4J” attack, when a user tries to log into a web-server, the web-server attempts to “log” all users attempting to access the system, using Apache Software Foundation logging-software. If a user uses HTTPS (i.e., HTTP over TLS), then the user’s TLS message will be decrypted, in order to allow the user to log into the web-server. The Apache logging-software will normally access another remote machine using Java code, to get more information about the user to log. In the “LOG4J” attack, the cyber-attacker will attempt to login using text that will direct the Apache logging-software to access a remote machine that the cyber-attacker controls, which will thus take control of the web-server being accessed. The attacker can take control of the entire secured web-server, yielding the unencrypted data for millions of other users.

Surprisingly, the use of HTTPS does not prevent the attack, for several reasons: (i) The attacker is not typically authenticated when using TLS (while the web-server is authenticated); (ii) The attacker’s message must be decrypted in TLS in order to perform the login; (iii) The use of TLS (in HTTPS) actually increases the likelihood that the cyber-attack will succeed, since the use of TLS encryption makes it impossible for layer-3 "Intrusion Detection Systems" (IDSs) to examine the encrypted HTTPS traffic, to try to detect potential cyber-attacks. (In an attempt to detect cyber-attacks, hardware IDS middle-boxes will run software that searches through vast amounts of Internet traffic, looking for "signatures" (i.e., a byte-sequences) of known cyber-attackers).

Table 4 illustrates the 10 largest global cyber-attacks reported to date, against a secured web-server that is open to the public. Yahoo was compromised by an external cyber-attacker in 2013, and 3 billion user accounts were compromised. Yahoo made HTTPS available on its mail servers in January 2013. One would expect that most of the service providers in Table 3 were using HTTPS by 2014, given Yahoo’s experience. However, it is clear that even with the wide-spread use of HTTPS and TLS (as in HTTP-over-TLS), large external cyber-attacks still occur frequently, where the data of 100s of millions of users is compromised.

In summary, according to Internet Society TLS provides "end-to-end security" of data sent between applications over the Internet, but this statement is imprecise. The "security" TLS achieves is "cryptographic-security", and it does not imply immunity to all types of layer-3 cyber-attacks. In contrast, TLS flows are vulnerable to many common layer-3 cyber-attacks. The previous discussion shows that TLS provides excellent "Secrecy" but provides relatively weak "Security" against general cyber-attacks, i.e., TLS provides excellent immunity to eavesdropping, message tampering and forgery, but provides little immunity to many common layer-3 cyber-attacks, especially DoS/DDoS flooding attacks, considered one of the most "powerful weapons on the Internet".

In contrast, the proposed SDD-IIoT / SDD-WANs eliminate all external IP-based cyber-attacks, for several reasons: (i) The SDD-WANs do not read or respond to the IP protocol or IP packet headers; (ii) A D-flow to an un-approved remote-machine will not be approved by the AC/AC system; (iii) Only approved D-flows between approved D-transceivers will be approved by the AC/AC system;

(iv) Any data transmitted by un-approved entities will be quickly detected and eliminated by the Guaranteed Intrusion Detection Systems, in real-time and in hardware.

Table 4. World's 10 Largest reported Cyber-Attacks (CSO Online, Nov. 2022).

Service	Date	Description	External / Internal
Yahoo	Aug. 2013	3 billion accounts	external
MySpace	2013	360 million accounts	external
Yahoo	2014	500 million accounts	external
Adult Friend Finder	Oct. 2016	412 million accounts	external
Aadhaar	Jan. 2018	1.1 billion accounts	external
Marriott International	Sept. 2018	500 million accounts	external
Facebook	April 2019	533 million accounts	internal
Alibaba	Nov. 2019	1.1 billion pieces of user data	internal
Sina Weibo	March 2020	538 million accounts	external
Linked In	June 2021	700 million accounts	external

2.2. TCP, TLS and HTTPS in the Deterministic Pillar

Five protocols in the Best-Effort pillar in Figure 1b receive "Best-Effort" services from IP. These five protocols are: TCP, UDP, TLS, HTTP, and HTTPS. These BE protocols are programmed into computer Operating Systems, such as Unix, Linux, Windows, and the Apple-OS, and these protocols must exist for decades into the future, to support legacy Best-Effort IoT software. Application programs in the Consumer-IoT can invoke these protocols at any time, without any pre-approval, and can typically send data to any other computer on the Internet, at any data-rate and at any time. This uncontrolled behaviour allows for congestion, BufferBloat and DoS/DDoS attacks in the Consumer-IoT.

The Deterministic pillar in Figure 1b must provide deterministic versions of these 5 protocols. These deterministic protocols are labelled as UDP*, TCP*, TLS*, HTTP*, and HTTPS* in Figure 1b. These deterministic protocols must not rely upon the Best-Effort IP; They must rely upon the AEDCs provided for M2M traffic flows in the SDD-WANs. Hence, computer Operating Systems such as Unix, Linux, Windows, and the Apple-OS, must offer software-interfaces for these 5 deterministic protocols. Any application programs in the Industrial-IoT wishing to use these deterministic protocols must first receive pre-approval from the AC/AC system, to establish a deterministic M2M traffic flow in the SDD-WAN(s) (i.e., an AEDC). Once a deterministic M2M traffic flow is established, an application program can send authenticated and encrypted data only to the pre-approved destination, at a pre-approved deterministic data-rate which cannot be exceeded. This behaviour is controlled by the AC/AC and eliminates congestion, BufferBloat and DoS/DDoS attacks in the Deterministic pillar.

2.3. Access-Control Systems

The poor cyber-security of the Consumer-IoT has lead to significant research over the last decade [52–61]. Much research has focussed on "Access-Control" systems, which limit access to critical resources, typically using AI rule-based policy engines [62–65]. In 2021, the US government issued an Executive Order 14028, entitled "Improving the Nation's Cybersecurity", which directed US industries to adopt the "Zero Trust Architecture" (ZTA) security model [66–68]. The ZTA is a rule-based Access-Control system, where rules control access to resources. Access to any resource, however small, requires approval from the system. Even the insertion of a memory stick into a computer system can require approval from the system. Access-Control systems can significantly-reduce the vulnerability to external and internal cyber-attackers, by adding rules to control access.

2.4. *Intrusion Detection Systems*

"Intrusion Detection Systems" (IDs) have become critical to secure the Consumer-IoT. These systems typically reside in a hardware "middle-box". They process traffic flows in a subnetwork, examining the byte-sequence in every traffic flow using "Deep Packet Inspection" (DPI), looking for "signatures" of a known cyber-attacker. According to Cisco, the Consumer-IoT transported about 9.1 billion Gigabytes of traffic/day in 2021. The latest IDSs employ "Artificial Intelligence" (AI), i.e., machine-learning (ML) and deep-learning (DL), to better detect cyber-attackers. The success-rates in detecting cyber-attacks can exceed 99%. Nevertheless, the amount of traffic to process each day is enormous, potentially billions of Gigabytes of traffic/day. Furthermore, the introduction of IDS middle-boxes significantly-increases the capital costs of the Consumer-IoT, and introduces cyber-security vulnerabilities, as IDS middle-boxes can be compromised by cyber-attackers. The US NIST has guidelines on IDSs [69,70]. IDSs are explored in [71–80].

2.5. *Cryptography*

2.5.1. Symmetric (Secret) Key Cryptography (SKC)

In SKC, the sender and receiver share a secret symmetric key, to encrypt and decrypt messages using Quantum-Safe ciphers. The need to share a secret key is a drawback, and motivates the "Public Key Cryptography" (PKC) described ahead. SKC is more efficient than PKC; it uses smaller keys, has stronger security, and faster computations. Popular SKC ciphers are the US Advanced Encryption Standard (AES) block cipher [81,82], and the Chacha20 stream cipher [50].

The US NIST defines several security levels for ciphers. The AES-256 security-level implies that a cipher is at least as hard to crack, as the AES cipher with a 256-bit key. Grover's quantum-search algorithm can crack AES, with a quadratic speedup. However, even with a super-conducting Quantum Computer, Grover's algorithm requires billions of years to crack AES-256 [41]. Hence, the NIST AES-256 security level is considered Quantum-Safe.

2.5.2. "Authenticated Encryption" (AE)

"Authenticated Encryption" was specified by NIST in 2003, and by the IETF in 2008. AE will both encrypt and authenticate a message. "Authenticated Encryption with Associated Data" (AEAD) also allows a message to contain an unencrypted (but authenticated) data field [83,84]. For proven security, encryption uses the Chacha20 cipher, and authentication uses a Poly1305 message authentication code [50]. AEAD is used in Google Chrome and FireFox web-browsers, and in TLS version 1.3. The SDD-WANs can also use AE/AEAD.

2.5.3. "Public Key Cryptography" (PKC)

Currently, PKC is used to secure most internet communications. In PKC, keys are generated in pairs, with a Public Key and a Private Key. A web-site advertises its Public Key to the world on a Web-Certificate, which contains a Digital Signature to ensure it cannot be altered. To connect to the web-site, a user uses the Public Key to encrypt its data. The web-site uses its Private-Key to decrypt the data. Unfortunately, Quantum Computers are expected to crack PKC by about 2030, leading to research on Quantum Resistant PKC [85,86].

2.5.4. Post-Quantum Cryptography (PQC)

In 2016, the US NIST started a project on PQC [87]. In 2017, NIST started a PQC Standardization Process, to standardize (i) public-key encryption algorithms, and (ii) digital signature algorithms. The final selections were made after 3 rounds of competition, in July 2022. Status reports on each round are available from the NIST and ETSI web-sites. The results of round 3 are presented at [88]. In the class of public-key encryption algorithms, the Crystals-Kyber submission was selected. In the class of digital signature algorithms, 3 submissions were selected: (i) Crystals-Dilithium, (ii) Falcon, and (iii) Sphincs+.

These PQC algorithms will be integrated into the IoT protocol suite, to ensure that the transport layer (i.e., TLS protocol) is cryptographically-secure, over the next several years [89]. However, as stated earlier, a cryptographically-secure TLS protocol is still vulnerable to layer-3 congestion, BufferBloat and DoS/DDoS attacks. A cryptographically-secure TLS protocol is unusable for the ultra-low-latency control-systems of critical infrastructure.

2.6. QoS Guarantees in the IoT

2.6.1. QoS Guarantees for Best-Effort Traffic

The problem of achieving QoS guarantees (on the delivery, latency and throughput) of competing traffic flows in the Internet is well-studied [90–94]. Two switch architectures for BE-IP routers are popular: (i) the "Input-Queueing" (IQ), and (ii) the "Combined Input and Output Queueing" (CIOQ) architectures. The design of packet buffers for Internet routers is explored in [95,96].

The scheduling of multiple BE traffic flows through an IQ or CIOQ switch, to achieve fair service, is a well-studied problem [97], [98]. The scheduling problem can be viewed as a matching problem on a bipartite graph. It has been established that a "Maximum Weighted Matching" (MWM) algorithm can achieve 100% throughput in an IQ or CIOQ switch, but the algorithm is too complex for practical implementations.

In practice, the iSLIP scheduling algorithm is fast and yields good performance, and is used in many BE-IP routers. Under a random-uniform traffic model, iSLIP can achieve a throughput of 100% [98]. However, the delays can be large at high link loads. To lower queueing-delays, BE-IP routers are often "Over-Provisioned", i.e., they typically operate at peak loads well below 100%. According to Google, layer-3 links typically operate at loads between 20%-30% [99,100].

Over-provisioning in the Consumer-IoT results in a significant cost. A layer-3 BE-IP link with a capacity of 800 Gigabits-per-second (Gbps), operating at 25% utilization, will transport about 200 Gbps of traffic. Thus, about 75% of the link capacity is un-used. This un-used link capacity allows for traffic to be re-routed in cases of link failures or congestion, so it does provide benefits. In Section 7, it is shown that capital costs of this poorly-utilized excess capacity can reach US$100s of billions annually.

2.6.2. IEEE and IETF Activities for Improved QoS

The IETF had explored ways to achieve high "Quality of Service" (QoS) in the Internet in the 1990s, with the "Integrated Services" and "Differentiated Services" service models [101,102]. However, these IETF models were based on a "Best-Effort" communications paradigm, and did not provide deterministic services.

The IEEE 802.1 Working Group has presented a tutorial on a "Deterministic Ethernet" (D-Ethernet) network in 2012 [103]. The IEEE has proposed a "Time-Slotted Channel Hopping" (TSCH) technology for wireless networks in 2012 [104]. The TSCH proposal (IEEE-802.15.4e) amended the "Medium Access Control" (MAC) protocol within the IEEE "Low-Rate Personal Area Networks" (LR-PANs) standard 802.15.4. The IETF created a "Deterministic Networking" (DetNet) group, that has proposed a deterministic wireless network based upon TSCH in [105].

The DetNet group has also proposed a "Converged-WAN" that in principle could support both best-effort and deterministic traffic flows [106–108]. The DetNet Converged-WAN retains the 3 vulnerabilities that have existed in IP networks for many decades: it uses: (i) unencrypted and (ii) un-authenticated IP packet headers, and (iii) middle-boxes. Huawei has also reported a deterministic IP network in [109]. It also uses: (i) unencrypted and (ii) un-authenticated IP packet headers, and (iii) middle-boxes. These networks are thus vulnerable to layer-3 cyber-attacks, i.e., Spoofing cyber-attacks (in which an un-encrypted IP packet header is modified) and DoS/DDoS cyber-attacks.

2.6.3. The Search for Ultra-Low-Latency Layer-3 Networks

According to Akamai, the design of an Internet that operates at the "Speed of Light" could transform IoT services [110]. The IEEE has developed a list of desirable features for an ultra-low-latency "Tactile Internet" [111]. The IEEE has proposed "Time Sensitive Networks" (TSN) as a step towards achieving ultra-low-latency networks [51].

One challenge to achieving ultra-low-latency in the Consumer-IoT in the past was the following theoretical problem: The best known algorithms for scheduling deterministic traffic flows through deterministic packet switches could not achieve 100% throughput, with bounded latency and jitter guarantees, while requiring only unity speedup (see next subsection). In other words, there was no known scheduling algorithms to achieve the desired goals.

2.6.4. Birkhoff-von-Neumann (BVN) Stochastic Matrix Decomposition

A theoretical frame-work for scheduling deterministic traffic flows through an IQ crossbar switch is given by the "Birkhoff-von-Neumann" (BVN) stochastic matrix decomposition algorithm [112]. Consider an NxN switch using an IQ or CIOQ switch architecture. The deterministic traffic rates for N^2 traffic flows between all pairs of input and output ports are specified in an NxN "Traffic Rate Matrix" T. Assume a repeating (periodic) scheduling-frame with a length of F time-slots, for some integer F. The deterministic rate of traffic between input and output ports (j,k) is given by T(j,k), can be expressed as a fraction of the data-rate that can be supported by an input (or output) port in F time-slots. A valid matrix T is "doubly stochastic", i.e., the sum of elements in any row of T must be ≤ 1.0, and the sum of elements in any column of T must be ≤ 1.0.

The BVN decomposition has 2 main steps [112]:

- Decompose the traffic rate matrix T into a series of P permutation matrices, each with a weight (i.e., probability of occurrence). The proof that this step can be accomplished is due to Birkoff and von Neumann (published in 1946).
- Schedule the P permutation matrices to appear in a periodic (repeating) scheduling-frame with F time-slots, for some integer F, such that the N^2 deterministic traffic rates specified in matrix T are satisfied, and some performance goals are achieved. Performance goals may include minimizing the average delay, minimizing the worst-case delay, or minimizing the length of the scheduling-frame F.

A deterministic crossbar switch using the BVN algorithm to schedule traffic in an IQ architecture was first proposed in 2001 [112]. It has a computational-complexity (runtime) of $O(N^{4.5})$ time, the length of the scheduling-frame F is $O(N^2)$ time-slots, and the maximum "service-lag" is $O(N^2)$ time-slots. The "service-lag" is defined as the deviation in service a flow receives, relative to a perfectly-scheduled flow with the same deterministic traffic rate in the same scheduling-frame. The problem of minimizing the length of the scheduling-frame F is known to be NP-Hard.

Several prominent research groups have improved the performance bounds of BVN deterministic switches over time. According to researchers at MIT, "the worst-case delay can be very high" with BVN decomposition, and "a higher (possibly much higher) rate than the long term average rate of a bursty, delay sensitive traffic stream must be allocated in order to satisfy its delay requirement". Researchers at MIT thus proposed adding a speedup to the BVN switch, to mitigate the worst case delay problem [113]. According to researchers at Bell Laboratories, "it is possible to derive bounds on jitter, but it is not possible to ensure that the jitter is low". The BVN algorithm results in "poor jitter performance, especially when there is a large number of ports in the switch" [114]. Researchers at UC Riverside established a jitter bound that grows with the switch degree $O(N)$, and stated an open problem on BVN scheduling of deterministic traffic: "to determine the minimum speedup required to provide hard guarantees, and whether such guarantees are possible at all" [115].

2.6.5. The SDD-IIoT

The theory for a "Deterministic IIoT" (D-IIoT) network which supports deterministic traffic flows with strict QoS guarantees (i.e., ultra-low latency and jitter guarantees) without speedup was presented in [117–119]. The "Deterministic IIoT" can achieve 100% throughput for deterministic traffic flows in a network of IQ or CIOQ switches, achieving ultra-low-latency and ultra-low jitter guarantees, while requiring no speedup. Additional results were reported in [120,121].

The Deterministic IIoT uses an innovative algorithm to decompose a BVN traffic rate matrix T, called the "Recursive Fair Stochastic Matrix Decomposition" (RFSMD) algorithm [42,117]. The RFSMD algorithm will decompose a doubly-stochastic traffic rate matrix T, into a sequence of permutation matrices, given a periodic (repeating) scheduling-frame of length F time-slots, such that every packet is delivered with ultra-low-latency and with near-perfect ultra-low jitter guarantees, while requiring no speedup (i.e., the speedup = 1). This RFSMD algorithm is the first known algorithm to decompose a BVN traffic rate matrix, to yield provable optimal-order deterministic delay and jitter guarantees [42,117]. This RFSMD algorithm results in the ultra-low-latency of the D-IIoT (please see Figure 5 in section VI).

A "Deterministic IIoT" was also explored in [43], where it was reported that determinism could reduce layer-3 buffer-sizes by a factor of 1000+ times, reduce end-to-end delays to the speed-of-light in fiber, and could reduce layer-3 capital costs by US$10s of billions/year. Additional results were reported in [42,44,45].

A Deterministic IIoT in which the routing and scheduling functions are migrated into the SDN control-plane was proposed in [123]. This migration eliminated 3 cyber-security vulnerabilities that have existed in the Consumer-IoT for decades: the use of (i) unencrypted IP packet headers, (ii) un-authenticated IP packet headers, and (iii) middle-boxes. The elimination of these cyber-security vulnerabilities could then improve cyber-security in the IoT, as proposed in [124].

2.7. FPGAs with Terabits of IO Capacity

A conventional BE-IP router suffers from interference, congestion and BufferBloat. As a result of BufferBloat, a BE-IP router with a capacity of several Terabits-per-second (Tbps), will require buffers for 10s...100s of millions of packets. It is thus impossible to fit a conventional BE-IP router onto a single Integrated Circuit, either an "Application Specific Integrated Circuit (ASIC)", or a "Field Programmable Gate Array" (FPGA).

A BE-IP router typically uses the "Bandwidth-Delay-Product" (BDP) buffer-sizing rule of thumb, to determine buffer sizes. A transmission link with a capacity of 4 Tbps and an end-to-end delay of 250 milliseconds will require a worst-case buffer-size of $\approx$ 1 terabit of memory. Assuming an average IP packet size of 1,000 bytes, the transmission link requires a worst-case buffer-size of $\approx$ 125 million BE-IP packets. It is thus impossible to fit a BE-IP router with a capacity of several Tbps onto a single ASIC or FPGA.

However, it has been shown that the use of determinism can eliminate "BufferBloat" and reduce buffer-sizes by a factor of $\approx$ 100,000+ times [41,45]. The same transmission link, using determinism, may require a worst-case buffer for $\approx$ 1,250 packets. Hence, a simple authenticated D-switch can be created using a single ASIC or FPGA.

D-switches offer a dramatic reduction in complexity, compared to a layer-3 BE-IP router, and they are well-suited for fabrication using ASICs or FPGAs.

- (1) The tasks of routing and scheduling of D-flows have been removed from layer-3, and have been migrated to the SDN control-plane;
- (2) Deterministic communications can reduce worst-case buffer sizes by a factor of 100,000-1,000,000 times [41–43,45];
- (3) D-switches do not need Gigabytes of high-speed RAM to store insecure layer-3 routing tables;
- (4) D-switches do not need a processor or a Linux operating system running the insecure layer-3 "Berkeley Sockets" software to implement insecure layer-3 protocols such as BGP.
- (5) D-switches are also much easier to secure, compared to a layer-3 BE-IP router.

- (6) One-Time-Programmable FPGAs can also be used to improve security, as their functionality cannot be modified.

2.7.1. The Intel Stratix FPGAs

The Intel Stratix 10 TX FPGA was introduced in 2018. It is fabricated with a 14 nanometer tri-gate CMOS technology. One FPGA supports computations at 9 TeraFlops/sec, and has a peak IO bandwidth of ≈ 3.5 Tbps (with 60 electrical transceivers operating at 57.8 Gbps each). The price is ≈ $7,500 USD per FPGA. A D-switch with ≈ 3.5 Tbps capacity can fit on one FPGA, and consume $\leq$ 225 watts.

In comparison, a Cisco CRS-3 ("Carrier Router System") BE-IP router cabinet that was commercially-available in 2015 had a capacity of 4.5 Tbps, occupied 56 cubic feet of volume, weighed 1,630 pounds, and used 7.66 kW of power. These FPGAs have only been available since 2018, and provide an unprecedented opportunity for innovation and cost-reduction in layer-3.

3. The Deterministic IoT - Key Features

3.1. Secured Components

The proposed "Deterministic IIoT" supports multiple deterministic SDD-WANs in a new forwarding sub-layer 3a, and utilizes several types of secured components:

- Deterministic Traffic Sources (D-sources)
- Deterministic Traffic Sinks (D-sinks)
- Deterministic Transceivers (D-transceivers), with a D-source and D-sink
- Deterministic Packet Switches (D-switches)
- The SDN Control-Plane

The SDN Control-Plane implements an "Admission-Control/Access-Control" system to control access to network bandwidth. This AC/AC system is organized hierarchically into several types of collaborative AI rule-based "Zero Trust Architecture" controllers, (also called "Attribute-Based Access Control" (ABAC) Systems):

- IIoT-Controller
- WAN-Controllers
- Enterprise-Controllers

These controllers will provide the repository for the large number of rules and attributes (i.e., the "knowledge base") used in each ZTA controller (please see ahead).

3.2. Deterministic Schedules (D-schedules)

The concept of a "Deterministic Schedule" (D-schedule) is critical to enable the fine-grain access-control to network bandwidth. Define a D-schedule for a directional-link in the SDD-WAN, as a periodic (repeating) schedule, valid for a "Scheduling-Frame" that comprises many time-slots. The D-schedule will specify which D-flows (if any) have reservations to transmit data over the given directional-link, for the time-slots in the scheduling-frame. (A D-flow is also called an "Authenticated Encrypted Determinisitic Channel".) All the D-schedules for an SDD-WAN collectively define the times in which authorized data-transfers may occur in the SDD-WAN. Any data-transfers occurring at any other times represent anomalies, i.e., malicious packets from an external cyber-attacker. Hence, the D-schedules effectively define many "Guaranteed Intrusion Detection Systems" (G-IDSs), where any un-authorized transmission is easily detected in hardware.

3.3. Deterministic Transceivers

The D-transceivers enforce the fine-grain access-control to the bandwidth of an SDD-WAN. They implement 2 important control-policies missing in the existing Consumer-IoT: (i) "Admission-Control/

Access-Control", and (ii) "Rate-Control"". A secured-computer can only access the bandwidth of the SDD-WAN using D-transceivers, after receiving approval from the SDN control-plane. The D-transceivers provide hardware-enforcement of the access-decisions of the collaborative ZTA controllers.

A D-source receives a list of approved D-flows, each with a reserved deterministic (or "Guaranteed-Rate") of transmission, from the control-plane. For each approved D-flow, the D-source maintains a Quantum-Safe key for "Authenticated Encryption". The SDN control-plane provides a D-schedule to the D-source over a secured D-flow, which identifies the time intervals within a periodic scheduling-frame, in which approved D-flows have reservations to transmit data from the D-source. A D-sink receives a list of approved D-flows, each with a reserved deterministic of reception, from the control-plane. For each approved D-flow, the D-sink maintains a Quantum-Safe key for the decryption process of AE. The SDN control-plane forwards a D-schedule to the D-sink over a secured D-flow, which identifies the time intervals within a period scheduling-frame, in which D-flows have reservations to transmit data to the D-sink.

3.4. IP Packet Fragmentation

A D-flow transmits one data stream from a D-source to a D-sink, over an "Authenticated Encrypted Deterministic Channel". The AEDC is "data-agnostic", i.e., it can transport IP data, video-data, encrypted TLS data, or any other type of data. In most cases, devices will transmit IP data. IP packets have variable sizes, with up to 64 Kbytes when using the IPv6 protocol. The D-sources can partition larger packets into smaller "cells" (with $\approx$ 1 Kbytes each), for transmission in sub-layer 3a, and the D-sinks can re-assemble the larger packets. (Each cell must pass an "Authorization-Check" explained ahead, and will thus need a sequence number and a CRC checksum for error detection.)

3.5. Deterministic VPNs

Figure 3a illustrates many BE-IP routers in layer 3, and many D-switches (i.e., FPGAs) in sub-layer-3a. Figure 3b illustrates an SDD-WAN spanning the European Union, with 28 nodes (cities) and 82 edges. In Figure 3a, each city has one D-switch, with fiber-optic edges to its nearest neighbours (other D-switches). In Figure 3b, the solid black lines represent fiber-optic edges between cities, and the dotted lines represent ultra-low-latency D-flows between cities. The existence of a programmable forwarding-plane for D-flows in sub-layer-3a will alter the network topology seen by a BE-IP router in layer-3, thus improving layer-3 efficiency and security.

Two BE-IP routers in layer-3 can each be assigned D-transceivers, so that they can access sub-layer-3a, under the control of the SDN control-plane. These two routers will view a D-flow as a dedicated deterministic connection with a deterministic data-rate. Packets transmitted on a D-flow will bypass many intermediate BE-IP routers in layer-3, as they traverse the ULL D-switches in sub-layer-3a of the SDD-WANs instead. Hence, D-flows can also be used to interconnect BE-IP routers, under the control of the SDN control-plane, with ULL deterministic connections which are immune to layer-3 cyber-attacks.

A "Deterministic Virtual network" (DVN) is a collection of D-flows, under the control of a single administrative entity, i.e., an "Enterprise". DVNs are isolated and completely independent from one another. The traffic within DVNs is "interference-free", as a result of the AC/AC system in the SDN control-plane. Within a DVN, traffic can: (a) remain unencrypted, or (b) it can be completely encrypted. An encrypted DVN is called a "Deterministic Virtual Private Network" (i.e., a D-VPN).

In Figure 3b, 2 D-VPNs are embedded into the network. Two cities, Madrid and Stockholm, each have a D-VPN which interconnects the specified city to every other city in the EU SDD-WAN. Specifically, each city has a D-VPN with 27 D-flows, with one D-flow to every other city in the EU network. A D-VPN with 27 D-flows originating at Madrid and directed to every other city is shown by the RED dotted lines in Figure 3b.

3.5.1. The "Admission-Control/Access-Control" (AC/AC) System

The Deterministic pillar utilizes an AC/AC system, to control access to network bandwidth. The AC/AC system in the SDN control-plane is composed of many smaller collaborating ZTAs, to comply with US Executive Order 14028 [66]. Each ZTA is actually an "Attribute-Based Access-Control System" (ABAC-system) [64,65], in which access to any resource, however small, requires user authentication.

The ZTA includes the following components [64,65]: (a) A set of objects, wherein each object has a list of attributes; (b) A set of requestors, each capable of requesting access to objects; (c) A set of rules in the form of "if...then" clauses; (d) A "Policy-Engine", to read the rules, perform logical deductions and determine the access-control decisions, i.e., ultimately approve or deny the requests for access to an object; and (e) A set of "Policy Enforcement Points", i.e., devices which enforce the access-control policy decisions. A ZTA is basically an AI rule-based "Expert System", which implements the rules which control access to resources in the SDD-IIoT. The "Knowledge Base" of a ZTA controller consists of the sets (a), (b) and (c).

The AC/AC system in the SDN control-plane has a hierarchical organization, with three types of Collaborative AI rule-based Controllers:

- the IoT-Controllers, the WAN-Controllers, and the Enterprise-Controllers

The IoT-Controller stores the Knowledge Base required to maintain approved D-flows between multiple SDD-WANs in the SDD-IIoT. The IoT-Controller can be managed by a consortium of service-providers, or the government.

A WAN-Controller maintains the Knowledge Base needed to manage approved D-flows between multiple enterprises within one SDD-WAN. It is managed by the WAN service-provider, i.e.., a company such as Google or Microsoft. Each Enterprise-Controller maintains the Knowledge Base that each enterprise requires to manage its own resources, i.e., network bandwidth, software systems and hardware systems. It may includes the following objects, each with its associated attributes:

- Employees; Secured-Computers; Secured-Databases;
- D-Transceivers; DVNs; D-VPNs;

Typically, the list of attributes for an employee may include: a name and employee number, an address, a cell-phone number for dual-factor authentication, and biometric data, i.e., a picture for facial recognition; a "finger-print", a "voice-recording" for voice-recognition; one or more passwords or hashes of each password, the employee's speciality, the Department to which the employee belongs; bits denoting the employee's permission to access and update the Knowledge Base; and a list of secured-resources (i.e., secured-computers and secured-databases) which the employee can access. Similarly, secured-computers and secured data-bases have many attributes, which can be used within the rules to control access. The use of AI-based ZTAs with biometric data will also significantly reduce the number of successful internal cyber-attacks. (Please see [41] for details.)

3.6. Authorization-Check

Every packet in a D-VPN must pass an "Authorization-Check", after it is received at a D-sink. Each packet has an "Authorization-Token" with A bits (where A $\approx$ 256 - 1024 bits), that identifies the packet as valid. The Authorization-Check performs the decryption process and authentication for the AE algorithm performed on all packets in a D-VPN. By performing the Authorization Check, a D-transceiver implements a "Policy-Enforcement Point" for the ZTA-controller, and it implements the Guaranteed Intrusion Detection System.

We describe a simple Authorization-Check. The IETF standard for AE uses the Chacha20 stream cipher for encryption, with a 512 bit key, and a Poly1305 "Message Authentication Code" (MAC) for authentication [83,84]. In addition, each D-source can maintain a counter with $\approx$ 64 bits which records its "current-time", i.e., the time elapsed since the D-source was last 'reset' by the SDN control-plane. Each tick of current-time could represent 10-20 nanoseconds. (A 64-bit counter could last for 1,000 of years.) An Authorization-Token can consist of a current-time stamp, plus a 16-bit sequence number. The sequence number is used when large IP packets are fragmented into smaller cells before transmission.

For a malicious packet to pass the Authorization-Check, an external cyber-attacker must perform several steps: (a) successfully crack the Quantum-Safe AE cipher used to encode a D-flow; (b) access the fiber, and overwrite a legitimate packet for the D-flow with a malicious packet, with a valid Authorization-Token, at the right time and on the right fiber. However, it will take billions of years for a superconducting Quantum Computer to crack the Quantum-Safe AE ciphers, assuming a security level of at least AES-256. Hence, the probability a malicious packet from an external cyber-attacker can pass the Authorization-Check is zero.

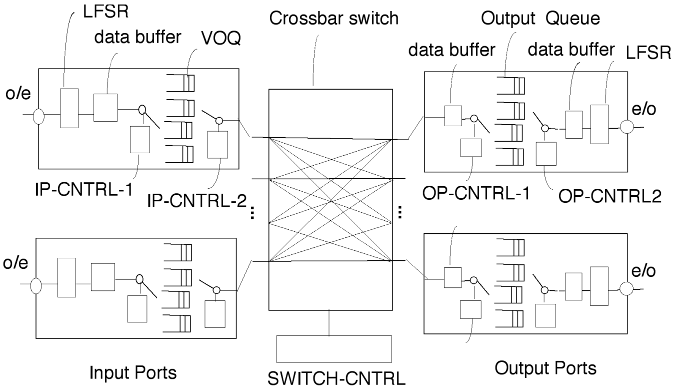


Figure 3. A CIOQ D-switch with 5 deterministic controllers.

3.7. The D-Switch - CIOQ Architecture

Many BE-IP routers use a "Combined Input and Output Queues" (CIOQ) switch architecture. A D-switch using CIOQ architecture is shown in Figure 4. We assume a discrete-time deterministic packet switch, which transfers data in time-slots, with F time-slots in a periodic (repeating) scheduling-frame.

The D-switch has N "input ports" (IPs) and N "output ports" (OPs). Each input port j has N "Virtual Output Queues" (VOQs). Each VOQ(j,k) buffers packets that arrive at input port (j) and depart on output port (k). Each output port k has N "Output Queues" (OQs), where OQ(j,k) buffers packets which arrives at input port (j) and depart on output port (k).

The NxN D-switch in Figure 4 has 5 controllers: (i) IP-CNTRL-1 directs incoming packets at each IP, to one VOQ. (ii) IP-CNTRL-2 selects data from a specific VOQ, to forward to one OP. (iii) OP-CNTRL-1 directs data arriving at a OP to one OQ. (iv) OP-CNTRL-2 selects data to transmit onto a fiber from one OQ. (v) The SWITCH-CNTRL connects N input ports to N output ports in each time-slot in the scheduling-frame, to meet the deterministic data-rate requirements of all D-flows supported by the switch.

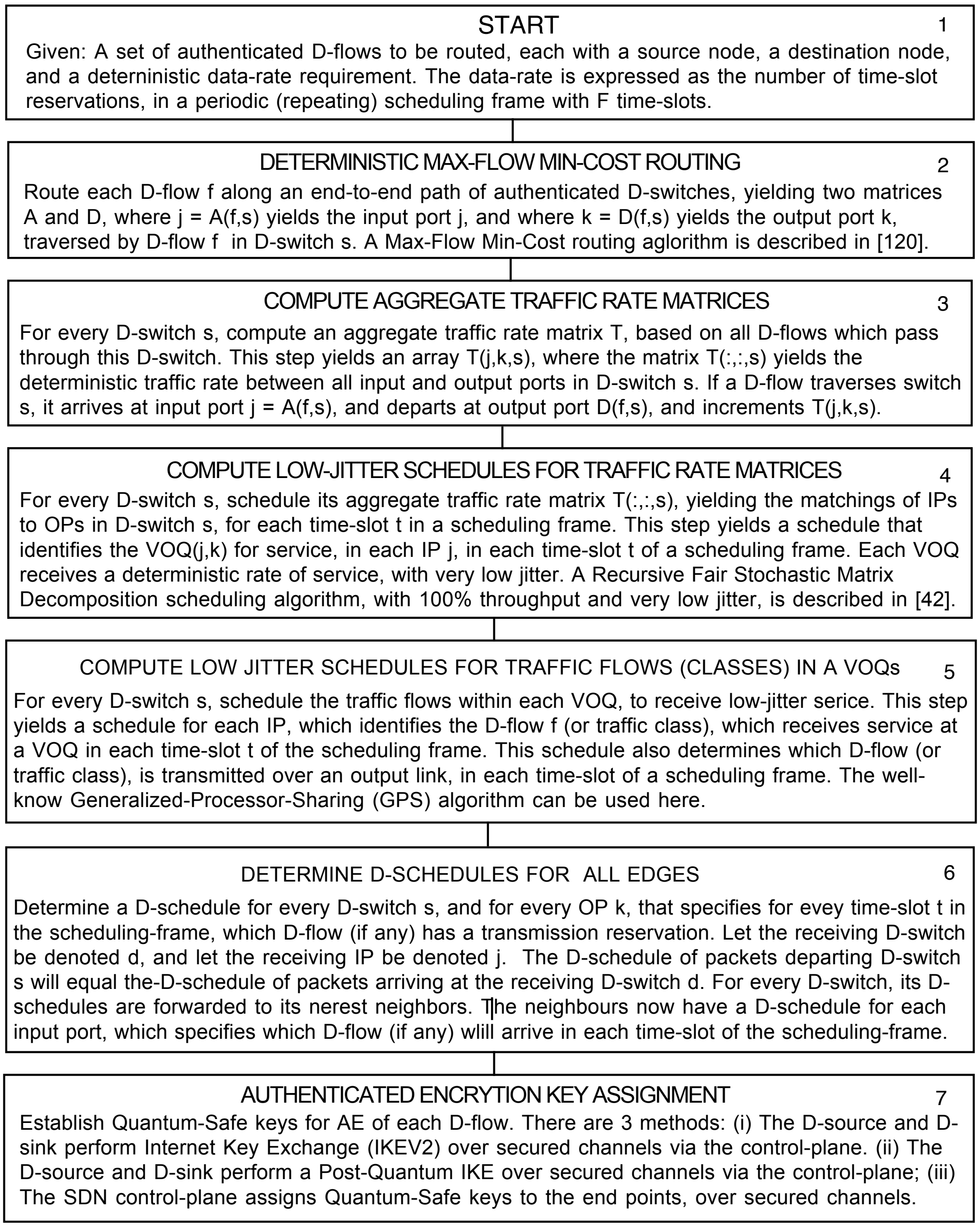
In Figure 4, all of the controllers can use D-schedules which are pre-computed in the SDN control-plane. D-switches do not process unencrypted and un-authenticated IP packet headers to make layer-3 routing or scheduling decisions. The D-schedules can be stored in high-speed lookup-tables. As a result of the pre-computed routing and scheduling, the D-switches remove much unnecessary hardware compared to a BE-IP router [41]: (a) several Gigabytes of expensive, high-speed RAM (memory) for insecure layer-3 routing tables; (b) a processor/Linux operating system running the insecure "Berkeley Sockets" layer-3 software; (c) a processor/Linux operating system for insecure layer-3 protocols, i.e., BGP, which add significant costs and security vulnerabilities to a BE-IP router.

3.7.1. Configuring the D-switches and D-transceivers

In the proposed SDD-IIoT, the SDN control-plane performs the routing and scheduling of packets for a newly-admitted D-flow in advance. Typically, an Enterprise-Controller will request a new D-flow from the WAN-Controller. The WAN-Controller will examine its knowledge-base, to see if one (or more) rules exist to approve the D-flow. If the request is approved, then the SDN control-plane will perform several task for the new D-flow. It will pre-compute: (i) the end-to-end routing; (ii) the end-to-end scheduling; (iii) the D-schedules for all traversed edges; (iv) the Quantum-Safe keys for AE of the D-flow. The SDN control-plane will then download control information to the SDD-WAN. The SDN control-plane is described in Section 4.

3.7.2. Synchronization

In the proposed SDD-IIoT, each D-switch can be "loosely synchronized" with its nearest neighbours [41]. Each D-switch receives a "Start-of-Frame" (SOF) signal (or encrypted packet) from each nearest neighbour, which identifies the start of a repeating scheduling-frame. A D-switch might receive a SOF signal/packet from each neighbour roughly once every millisecond (depending upon the duration of a scheduling-frame).



START 1

Given: A set of authenticated D-flows to be routed, each with a source node, a destination node, and a deterninistic data-rate requirement. The data-rate is expressed as the number of time-slot reservations, in a periodic (repeating) scheduling frame with F time-slots.

DETERMINISTIC MAX-FLOW MIN-COST ROUTING 2

Route each D-flow f along an end-to-end path of authenticated D-switches, yielding two matrices A and D, where j = A(f,s) yields the input port j, and where k = D(f,s) yields the output port k, traversed by D-flow f in D-switch s. A Max-Flow Min-Cost routing aglorithm is described in [120].

COMPUTE AGGREGATE TRAFFIC RATE MATRICES 3

For every D-switch s, compute an aggregate traffic rate matrix T, based on all D-flows which pass through this D-switch. This step yields an array T(j,k,s), where the matrix T(:,:,s) yields the deterministic traffic rate between all input and output ports in D-switch s. If a D-flow traverses switch s, it arrives at input port j = A(f,s), and departs at output port D(f,s), and increments T(j,k,s).

COMPUTE LOW-JITTER SCHEDULES FOR TRAFFIC RATE MATRICES 4

For every D-switch s, schedule its aggregate traffic rate matrix T(:,:,s), yielding the matchings of IPs to OPs in D-switch s, for each time-slot t in a scheduling frame. This step yields a schedule that identifies the VOQ(j,k) for service, in each IP j, in each time-slot t of a scheduling frame. Each VOQ receives a deterministic rate of service, with very low jitter. A Recursive Fair Stochastic Matrix Decomposition scheduling algorithm, with 100% throughput and very low jitter, is described in [42].

COMPUTE LOW JITTER SCHEDULES FOR TRAFFIC FLOWS (CLASSES) IN A VOQs 5

For every D-switch s, schedule the traffic flows within each VOQ, to receive low-jitter serice. This step yields a schedule for each IP, which identifies the D-flow f (or traffic class), which receives service at a VOQ in each time-slot t of the scheduling frame. This schedule also determines which D-flow (or traffic class), is transmitted over an output link, in each time-slot of a scheduling frame. The well-know Generalized-Processor-Sharing (GPS) algorithm can be used here.

DETERMINE D-SCHEDULES FOR ALL EDGES 6

Determine a D-schedule for every D-switch s, and for every OP k, that specifies for evey time-slot t in the scheduling-frame, which D-flow (if any) has a transmission reservation. Let the receiving D-switch be denoted d, and let the receiving IP be denoted j. The D-schedule of packets departing D-switch s will equal the-D-schedule of packets arriving at the receiving D-switch d. For every D-switch, its D-schedules are forwarded to its nerest neighbors. The neighbours now have a D-schedule for each input port, which specifies which D-flow (if any) wlill arrive in each time-slot of the scheduling-frame.

AUTHENTICATED ENCRYTION KEY ASSIGNMENT 7

Establish Quantum-Safe keys for AE of each D-flow. There are 3 methods: (i) The D-source and D-sink perform Internet Key Exchange (IKEV2) over secured channels via the control-plane. (ii) The D-source and D-sink perform a Post-Quantum IKE over secured channels via the control-plane; (iii) The SDN control-plane assigns Quantum-Safe keys to the end points, over secured channels.

Figure 4. SDN Control-plane flow-chart.

4. The SDN Control-Plane

Figure 4 illustrates a flow-chart for the SDN control-plane, for an SDD-WAN using IQ or CIOQ switches. (The control-plane for crosspoint-buffered switches is similar.) This flow-chart upgrades an earlier flow-chart first presented in [41], to include Authenticated-Encryption and quantum-safe key assignment. The SDN control-plane will compute several deterministic schedules for each D-switch, to allow encrypted packets in a D-VPN to traverse the SDD-WAN. The D-switches do not use the IP protocol, and do not examine unencrypted IP packet headers to make layer-3 routing decisions. As a result, packets in D-flows can remain fully-encrypted from end-to-end, resulting in improved cyber-security. Specifically, these D-schedules define the time intervals when authorized packet transmissions may occur, on every edge in an SDD-WAN network.

The following notation will be used in Figure 4. The variable s will denote a D-switch, for $s \in [1...S]$. Let every D-switch have N input ports (IPs) and N output ports (OPs). Let j denote an IP. Let k denote an OP. Let f denote a D-flow. (For the scheduling-purposes, a traffic class with a deterministic data-rate is can be treated as D-flow with a deterministic data-rate.) Let F denote the length of a periodic scheduling-frame, in time-slots.

4.1. Max-Flow Min-Cost Routing of D-Flows

The SDN control-plane has a global view of each SDD-WAN network. In Figure 4 box 2, the SDN control-plane will route every D-flow along a fixed path of D-switches, from a D-source to a D-sink. The routing algorithm ensures that every edge has sufficient bandwidth to accommodate the new D-flow. This step identifies the D-switches traversed by a new D-flow, and the IP and OP traversed in each D-switch. Every D-flow f has a deterministic data-rate denoted R(f) to be satisfied. A "Maximum-Flow-Minimum-Cost" (MFMC) routing algorithm is used in the SDN control-plane [120]. The algorithm optimizes aggregate throughput and minimizes costs, and can achieve up to ≈100 % utilization of edges in sub-layer 3a. No other routing algorithm can achieve a higher throughput. (A negligible fraction of each edge's capacity is used for "Start-of-Frame" signals/packets).

4.2. Compute Aggregate Traffic Rate Matrices

In box 3, the SDN control-plane computes an aggregate traffic rate matrix $T(j,k)$ for each D-switch s. This matrix records the aggregate traffic demand between the input and output ports of each D-switch, resulting from potentially 1,000s of D-flows. This step yields a 3D array $T(j,k,s)$, where the 3rd index identifies the D-switch s. For each D-flow f traversing D-switch s, which arrives at input port j and departs at output port k, the matrix-element $T(j,k,s)$ is incremented by the deterministic data-rate $R(f)$.

4.3. Compute Low-Jitter Schedules for VOQs

In box 4, for every D-switch s the aggregate traffic rate matrix T is scheduled, to yield a low-jitter transmission schedule for each VOQ. The scheduling of deterministic traffic flows through an IQ or CIOQ switch to meet QoS guarantees has a long history (see section 2). The problem of scheduling traffic in an IQ or CIOQ switch to achieve maximum throughput and minimum jitter is known to be NP-hard.

The SDN control-plane uses a fast recursive scheduling algorithm for deterministic switches, called the "Recursive and Fair Stochastic Matrix Decomposition" (RFSMD) algorithm [42],[117]. Given an $N \times N$ doubly stochastic traffic matrix $T(j,k)$, this algorithm will compute a schedule consisting of F permutation-matrices, which realize the traffic demand in matrix T. The algorithm is very fast, requiring $O((NF)log(NF))$ time. The algorithm can achieve 100% throughput in sub-layer-3a, and a bounded and very low-jitter, i.e., it will reduce end-to-end delays to the speed-of-light in fiber (see section 6).

This scheduling yields a 3D array $Q(j,t,s)$, where $k = Q(j,t,s)$ identifies the $VOQ(j,k)$ at IP j of D-switch s that is scheduled to transmit, for each time-slot t of the scheduling frame. These schedules provide each VOQ with a very-low-jitter deterministic rate of transmission, that satisfies the mend in matrix T.

4.4. Compute Low-Jitter Schedules for D-flows

In box 5, the D-flows within each VOQ are scheduled for transmission on each OP k, in each D-switch s. The deterministic service that each VOQ receives in box 4 is allocated to the D-flows buffered within that VOQ in box 5. The well-known "Generalized Processor Sharing" (GPS) algorithm can be used in this step. Algorithms to schedule the D-flows within each VOQ are given in [42]. These scheduling algorithms also minimize the jitter, which will reduce queue sizes and end-to-end queueing delays.

For scheduling purposes, a traffic class with a deterministic data-rate on an IIoT link can be treated as a D-flow, in boxes 5, 6, and 7. Hence, a single transmission schedule can also support D-flows and traffic classes [42][122].

Within a VOQ, each traffic class can have its own class-queue, to buffer the packets of many D-flows. Hence, the use of traffic classes will simplify the queueing and scheduling [42]. For each D-switch s, box 5 yields an array $f = FLOW(j,t,s)$, where an active D-flow (or traffic class) f will receives service, at IP j of the D-switch s at time-slot t.

4.5. Compute D-schedules for D-switches

The $FLOW$ schedules computed earlier can be used to compute a D-schedule for each output port k of every D-switch, i.e., the schedule of which D-flows (and traffic classes), if any, which have transmission reservations on each OP k, in each time-slot of a periodic scheduling-frame. These D-schedules will significantly strengthen cyber-security, as the precise departure times of all packets of all approved D-flows on each output port of every D-switch are pre-computed and known in advance.

4.6. Forward D-schedules to Neighbours

Consider a D-switch s that sends data over output port k, to a D-switch d which receives data over input port j. The D-schedule computed for output port k of D-switch s will also become the D-schedule for input port j of receiving D-switch d. The SDN control-plane will thus forward the D-schedule from D-switch s (output port k), to D-switch d (input port j). A D-schedule can also identify the output port an arriving packet requires, which will allows encrypted packets to traverse a D-switch, without examining IP packet headers. Hence, D-switches do not need to examine IP packet headers, in order to make layer-3 routing decisions. (To determine the forwarding for packets in a traffic class, extra processing is needed.)

4.7. Authenticated Encryption (AE) Key Assignment

Each D-flow transmits encrypted and authenticated data between a D-source and D-sink. The Quantum-Safe keys for the AE algorithm must be determined. In the existing Consumer-IoT, secure keys between two layer-3 end-points are achieved using the "Internet Key Exchange version 2" (IKEV2) algorithm, over secured layer-3 connections (tunnels) which use "IPSec" and pre-shared secret keys [135]. Several methods can be used in the SDD-WANs: (i) The end-points can perform the IKEV2 algorithm, over secured channels via the SDN control-plane, similar to [135,136]; (ii) The end-points can perform a Post-Quantum key exchange algorithm, over the secured channels via the SDN control-plane, similar to [137]; (iii) The SDN control-plane can generate Quantum-Safe keys, and assign these to the end-points over secured channels [41].

4.8. Summary - SDN flow-chart

This flow-chart ensures that every edge in the SDD-WAN will receive a D-schedule, and that the two end-points of each approved D-flow will receive a Quantum-Safe key for Authenticated-Encryption. The D-schedules guarantee that every approved D-flow will receive its deterministic rate of transmission through the SDD-WAN. The D-schedules will also eliminate the need for:

- (1) D-switches to process unencrypted and un-authenticated IP packet headers to perform insecure layer-3 routing;
- (2) Many Gigabytes of high-speed RAM to store insecure layer-3 BGP ("Border Gateway Protocol") routing tables;
- (3) Each D-switch to contain a processor running a Linux operating system and the insecure Berkeley Sockets software, to maintain insecure layer-3 protocols such as ICMP ("Internet Control Message Protocol"), BGP, and IGP ("Interior Gateway Protocol");
- (4) Layer-3 "middle-boxes", which perform "Network Address Translation" (NAT) necessary for insecure layer-3 routing;

The use of pre-computed D-schedules results in a vast simplification of the D-switches. Packets in an approved D-flow can be completely encrypted at a D-source, and they can remain encrypted while they traverse the network from end-to-end.

4.8.1. Communications of the SDN control-plane

M2M D-flows for control-systems will typically last for long periods of time, i.e., days, weeks, months or years. The SDN control-plane can configure a permanent D-VPN specifically for the management/control of each SDD-WAN.

5. Security Properties of the Deterministic IIoT

This section summarizes the security properties of the proposed SDD-WANs

Property 1: Communications of Secured Components: The SDD-WAN consists of several secured-components (the D-transceivers, D-switches, and the SDN control-plane), which communicate over D-flows with Quantum-Safe ciphers, typically at security levels AES-256, AES-512 or AES-1024. It takes billions of years for a superconducting Quantum Computer to crack the AES-256 security level [41]. Hence, the probability that any secured-component can be compromised by an external cyber-attacker is effectively 0.

Property 2: Majority Voting in De-centralized SDN control-plane: The SDN control-plane realizes an Admission-Control/Access-Control system, using 3 types of AI rule-based ZTA controllers (the IoT-Controller, WAN-Controller, and Enterprise-Controller), typically implemented as software systems running in data-centers. A single control-system is vulnerable to performance and reliability issues [125,126]. For maximum reliability/availability, multiple copies of each system will execute in separate data-centers, and majority voting is used to confirm each decision, i.e., 3 out of 5 copies must agree to confirm a decision. (This property exploits the principles of redundancy of hardware and redundancy of information, described in [47].) Hence, the SDN control-plane can be logically viewed as a "centralized entity" that controls the SDD-WAN(s), but it is actually a highly-distributed system, running software on multiple data-centers, and using majority-voting to consolidate the results. It is highly-protected from natural disasters (i.e., hurricanes, earthquakes), terrorist-attacks (i.e., explosions/missile strikes), and cyber-attacks (i.e., information-based attacks which attempt to compromise the communications of any secured components).

Property 3: Only Authorized D-flows Reserve Bandwidth: A request for a new D-flow will only be approved if a rule in the WAN-controller's knowledge-base explicitly allows for the creation of the D-flow. If approved, the SDN control-plane will pre-compute several values for the new D-flow, i.e., the (i) routing, (ii) the scheduling, (iii) the D-schedules, and (iv) the Quantum-Safe secret keys for the "Authenticated Encryption" of the D-flow. A D-schedule for an edge in the SDD-WAN will define the time-slots in a periodic (repeating) scheduling-frame, in which the D-flow has a reservation to transmit data. Any data transmission in a time-slot for which no transmission reservation exists is an anomaly, i.e., a malicious packet from a cyber-attack. The anomaly is immediately detected by the FPGAs, reported to the SDN control-plane, and the data is not forwarded.

Property 4 - D-flows Reserve Guaranteed Data-Rates: Every D-flow will reserve a deterministic (or guaranteed) data-rate through a path of D-switches in a SDD-WAN, from a D-source to a D-sink. The deterministic data-rate equals a guaranteed number of time-slot reservations within a periodic scheduling-frame consisting of F time-slots. Assuming that: (i) fiber-optic links support a data-rate of 800 Gbps, (ii) 1 Kbyte packets are transmitted in each time-slot, (iii) a scheduling-frame comprises F=16K time-slots, then each time-slot requires $\approx$ 20.48 nanoseconds, and the scheduling-frame requires $\approx$ 0.672 milliseconds.

Property 5 - Routing/Scheduling can Achieve $\approx$ 100% Utilization: The SDN control-plane will route every D-flow along a fixed path of D-switches, using a "Max-Flow Min-Cost" routing algorithm [120], which can achieve $\approx$ 100% utilization in sub-layer 3a. The control-plane will determine a D-schedule for every edge in the SDD-WAN. Each D-schedule identifies the D-flow (or traffic class) with a transmission reservation, in each time-slot of the scheduling frame. Using the scheduling algorithms in [42], the D-schedules can be circularly-rotated and still minimize buffer sizes and queuing delays, so that the D-switches do not need to be tightly synchronized. In practice, each D-switch must recognize a *'Start-of-Frame'* signal/packet from each of its neighbours, roughly once every millisecond [41]. The size of the packet queues can be reduced by factors of about 100,000 - 1,000,000 times compared to a BE-IP router (see section 6), and the end-to-end queueing delays can be reduced to the speed-of-light in fiber.

Property 6 - D-flows use End-to-End Quantum-Safe Encryption: The packets of D-flows within a D-VPN are encrypted at the D-source using Quantum-Safe AE ciphers, and can remain fully encrypted as they traverse the SDD-WAN from end-to-end. The packet headers do not need to be examined at intermediate D-switches to make layer-3 routing decisions. This property solves several significant weaknesses of the BE-IP network: (a) The insecure "Border Gateway Protocol" (BGP) routing used in layer-3 is eliminated; (b) The insecure "Domain Name Servers" (DNSs) used in layer-3 routing are eliminated; (c) The use of unencrypted and un-authenticated IP packet headers in layer-3 is eliminated. These headers are insecure and vulnerable to manipulation by cyber-attackers. (d) The need for middle-boxes to perform "Network Address Translation" (NAT) is eliminated.

Property 7 - Authorization-Checks at D-transceivers: Every packet received at a D-transceiver must undergo an "Authorization-Check". The packet will be decrypted and authenticated, using the secret AE keys associated with the D-flow at the D-transceiver. If the packet fails the authorization-check, then the packet is not delivered to any secured-computer, and the SDN control-plane is immediately informed of the anomaly. In order for a malicious packet from an external cyber-attacker to pass the authorization-check, the cyber-attacker must crack the Quantum-Safe AE key(s) used to authenticate/encrypt the packet. Assuming the AE keys support security levels AES-256 and higher, then it takes billions of years for a superconducting Quantum Computer to crack the AE ciphers. Hence, the probability a malicious packet can pass an Authorization-Check is zero.

Property 8 - The Guaranteed Intrusion Detection System: The D-switches/D-transceivers implement a "Guaranteed Intrusion Detection System" in FPGA hardware, where any un-authorized or malicious packet from an external cyber-attacker is detected in real-time. Consider 2 cases. Case 1: A packet that is transmitted over an edge in the SDD-WAN, in a time-slot for which no transmission-reservation exists. This anomaly is immediately detected at the receiving D-switch/D-transceiver. That packet is not forwarded, and the SDN control-plane is immediately informed. Case 2: Suppose an external cyber-attacker has compromised the SDD-WAN fiber, and managed to overwrite a valid packet transmission with a malicious packet transmission. That malicious packet will be delivered to the ultimate destination D-transceiver. However, by Property 7, it will fail the Authorization Check and be detected. That packet is not forwarded, and the SDN control-plane is immediately informed.

Property 9 - Redundant Paths for Reliability: For mission-critical applications, each "primary" D-flow is replaced with multiple (i.e., R >= 3) redundant D-flows, within one SDD-WAN. Each redundant D-flow is routed over an "edge-disjoint" path, i.e.., it does not share any edges with the primary path or any of the redundant paths. Every packet logically transmitted over the primary D-flow is replaced with R packets, transmitted over the R redundant paths. A receiving D-transceiver will eliminate duplicate copies and keep one copy of each packet. This scheme is similar to the IEEE 802.1 TSN FRER ("Frame Replication and Elimination for Reliability") proposal used in layer-2 networks. It is also similar to the IETF DetNet PREOF ("Packet Replication, Elimination and Ordering Function") protocol used in layer-3. (Mission-critical applications may also use "Forward-Error Correcting" (FEC) codes.) In order for the transmission of a packet in a primary D-flow to fail, all R redundant transmissions of the same packet must fail. Equivalently, all R redundant paths in one SDD-WAN must fail simultaneously. (This property exploits the principles of redundancy of hardware and redundancy of information, described in [47].) The cost of providing multiple redundant paths in sub-layer-3a (using inexpensive D-switches) is much lower than the cost of providing multiple paths in layer-3 (using expensive BE-IP routers).

Property 10 - Redundant Paths for Cyber-security: The redundancy technique described in property 9, will also significantly improve cyber-security within one SDD-WAN. Let each independent path use an independent Quantum-Safe AE cipher. In order to insert an undetected malicious packet, a cyber-attacker must over-write R legitimate packets with R malicious packets, on R redundant paths within one SDD-WAN. In order to pass the R authorization checks, the cyber-attacker must also crack the R Quantum-Safe AE ciphers, used in these R redundant paths. However, it takes billions of years to crack even one AE-256 cipher. Hence, the use of redundant hardware paths and redundant information (packets) within one SDD-WAN will also significantly-improve cyber-security. (This property exploits the principles of redundancy of hardware and redundancy of information, described in [47].) The probability a cyber-attacker can insert an undetected malicious packet into an SDD-WAN, when R redundant paths are used, is effectively zero. The use of multiple independent SDD-WANs, managed by independent cloud services providers, will also further improve cyber-security (see property 11).

Property 11 - Protecting Critical Infrastructure: Each nation will protect its critical infrastructures shown in Table 1 from external cyber-attacks. Each nation will likely have multiple independent SDD-WANs, managed by independent service providers, such as Google or Amazon Web Services. The service providers can generate new revenue streams by offering SDD-WANs and D-VPNs, with ultra-reliable and ultra-low-latency communications, along with exceptionally cyber-security and with immunity to external cyber-attacks, as a new service.

For each M2M-flow for critical infrastructure, a service-provider could engage $S \geq 3$ independent SDD-WANs, and utilize $R \geq 3$ redundant edge-disjoint paths within each SDD-WAN. Each redundant path is protected with an independent Quantum-Safe AE cipher, with a security level of at least AES-256. Assuming all $R \cdot S$ paths are operational, an attempted cyber-attack is detected if any one of the $R \cdot S$ packets associated with the M2M-flow fails the authorization check. To insert an undetected malicious packet into an M2M D-flow, a cyber-attacker must overwrite R legitimate encrypted packets with R malicious packets, in each of S SDD-WANs, and pass all $R \cdot S$ authorization checks. (It is difficult if not impossible to associate one encrypted packet with any one M2M-flow, as transmissions are encrypted, so just finding $R \cdot S$ encrypted packets belonging to one M2M-flow in S SDD-WANs is virtually-impossible.) In order to pass all the authorization checks, the cyber-attacker must crack all $R \cdot S$ of the AE ciphers used. However, it is infeasible for a cyber-attacker to crack even one Quantum-Safe cipher, let alone $R \cdot S$ ciphers. It is impossible for a cyber-attacker to insert an undetected malicious packet into an M2M D-flow, assuming all paths are operational. The same argument applies if only some paths are operational. Hence, it is impossible for a cyber-attacker to insert an undetected malicious packet into an M2M D-flow, provided that at least one redundant path from the source to the destination is operational in the S independent SDD-WANs. The probability of a successful undetected external cyber-attack is zero, provided that at least one redundant path from the source to the destination is operational in at least one SDD-WAN.

Property 12 - Protection from Internal Cyber-Attackers: Internal cyber-attackers are defined as users who have obtained the secret keys or passwords needed to access a secured-system. Internal cyber-attackers can log into a secured-computer, and in absence of any other control-system, they could access critical resources and perform significant damage. To combat internal cyber-attackers, the US government implemented Executive Order 14028, which requires US industries to adopt the ZTA to control access to all critical resources [66].

Network managers can develop a knowledge-base of rules, to detect all internal cyber-attackers, including: (i) un-authorized users, and (ii) authorized users trying to perform un-authorized tasks. Un-authorized users can be detected and eliminated by using rules that exploit biometric data. Authorized users trying to perform un-authorized tasks can be detected and eliminated by using rules to explicitly identify what authorized users are allowed to do.

The performance of exceptionally-important tasks could have rules to require the approval of multiple senior-level approved-users, so that any one authorized user cannot compromise the system. For example, access to a secured-computer with "top-secret" information could require the approval of multiple senior-level users, each authenticated with biometric data. Hence, the use of ZTAs with a comprehensive knowledge-base of rules, is the best-known method to achieve exceptionally-strong protection against internal cyber-attackers.

5.1. QKD Networks versus the SDD-WAN

In principle, QKD ("Quantum Key Distribution") Networks can supply "perfectly-secret" keys between pairs of users, thus enabling "Perfect-Secret" communications. The "perfectly-secret" nature of the keys is guaranteed by the Laws of Physics. However, the US "National Security Agency" (NSA) does not recommend the use of QKD networks [86]. The "National Cyber Security Center" (NCSC) in the UK, and the "Agence National de la Securite des Systems d'Information" (ANSSI) in France also do not recommend the use of QKD networks.

The US NSA outlines 5 drawbacks to QKD networks, as shown in Table 4. Several papers have also discussed these drawbacks of QKD networks [127–131].

Problem 1: QKD Networks cannot Authenticate the Source: It is well-known that QKD networks require "classical authenticated channels" for control. According to NIST, QKD Networks cannot authenticate the source. External hardware must be added to authenticate the source, which is usually achieved using dedicated point-to-point links, along with Pre-Shared (secret) Keys (PSK) and Symmetric Key Cryptography (SKC). Post-Quantum Cryptography (PQC) can also be used. Hence, the security of QKD network is now limited by the security of SKC or PQC, i.e., the computational hardness of cracking SKC/PQC.

Problem 2: QKD Networks Vulnerable to Insider Attackers: As shown in Table 5, according to the US NIST, QKD networks are vulnerable to insider (internal) cyber-attackers. Internal cyber-attackers could compromise the trusted relays in a QKD network, to compromise the security of the QKD keys. As stated in Property 12, these insider attacks can be mitigated with an AC/AC system, using Zero-Trust-Architectures, to control which "insiders" are authorized to access the system, and what these insiders are authorized to do. Network managers can develop a knowledge-base of rules, to detect (i) un-authorized users, and (ii) authorized users trying to perform un-authorized tasks. Un-authorized users can be detected by using rules that exploit biometric data. Authorized users trying to perform un-authorized tasks can be detected by using rules to explicitly identify what authorized users are allowed to do. The administration/control of the AC/AC system typically requires PSK, along with SKC or PQC. Hence, the security of QKD network is again limited by the computational hardness of cracking SKC/PQC.

Table 5. US NSA - 5 Drawbacks of QKD Networks [86].

Drawback	Summary
QKD is a Partial Solution	QKD cannot authenticate the source. Authentication typically requires the use of "Pre-Shared secret Keys" and SKC.
Special-Purpose Equipment	QKD relies upon unique physical layer communications, i.e., dedicated point-to-point fiber connections, or satellite communications.
Insider (Internal) Cyber-Attacks	QKD requires trusted relays, which increases costs and security risks from insider cyber-attacks. This prospect eliminates many use-cases of QKD.
Validating QKD is a Challenge	Security of QKD is limited by constraints of hardware & engineering designs. Tolerance for design errors is orders of magnitude smaller than for traditional systems. Several commercial QKD systems have been attacked.
Denial of Service (DoS) Attacks	QKD is sensitive to eavesdroppers (i.e., "photon number splitting attack"), and "Denial of Service" (DoS) attacks are a significant risk for QKD systems.

Problem 3: QKD Networks Vulnerable to DoS/DDoS Attacks: As shown in Table 5, according to the US NIST "there is no known way to prevent a flooding DoS attack against hosts visible on the Internet". As shown in Table 5, according to the US NIST, even QKD networks are vulnerable to DoS flooding attacks. According to the industry, DoS/DDoS attacks have been called "one of the most powerful weapons on the Internet". QKD networks are vulnerable to such attacks, to prevent the perfectly-secret keys from being delivered. Even TLS-flows in the Consumer-IoT, using perfectly-secret keys from a QKD network, are vulnerable to layer-3 DoS/DDoS attacks. According to [128], the vulnerability of QKD networks to DoS/DDoS attacks has no clear defense.

Problem 4: QKD Networks will require Software "Key Management Systems": A "Key Management System" (KMS) will allow for the scaling upwards, from small link-to-link quantum key generation systems, towards large-scale quantum key distribution networks [132,133]. The ETSI is working to define standards for the KMS and the software interface to access the KMS and keys. The administration/control of these software systems typically requires pre-shared secret keys, along with SKC or PQC. Hence, the security of QKD network is again limited by the computational hardness of cracking SKC/PQC.

SDD-WANs Can Support QKD Networks: Prior to this paper, there is no known multi-user layer-3 WAN with immunity to external cyber-attacks, which can provide "authenticated classical channels" to control QKD networks. The SDD-WANs proposed in this paper can thus enable QKD networks, by providing the "classical authenticated channels" needed for the control of QKD networks, in a programmable layer-3 network which is immune to external cyber-attacks.

SDD-WANs versus QKD Networks: In practice, the security of QKD networks is strongly limited by the drawbacks shown in Table 5. It is said that "a chain is as strong as its weakest link", and the use of QKD networks entails several "weakest links" shown above. The security of the QKD network is limited by: (i) The cryptography used to authenticate the source (i.e., SKC/PQC); (ii) The cryptography used to administer/control the AC/AC system, necessary to control internal cyber-attackers (i.e., SKC/PQC); (iii) The cryptography used to administer/control the AC/AC system, necessary to control the vulnerabilities to DoS/DDoS flooding attacks against QKD networks (i.e., SKC/PQC); (iv) The cryptography used to administer/control the AC/AC system, necessary to control the Key Management System (i.e., SKC/PQC). For these reasons, the US NSA, the UK NCSC and the France ANSSI do not recommend the use of QKD networks.

Fortunately, the use of SDD-WAN can address all 4 of these problems, by adding an AC/AC system, and thus the SDD-WANs can enable/support the use of QKD networks. However, given these vulnerabilities and given that the security of QKD networks is now limited to the computational hardness of cracking SKC/PQC due to several "weakest links", one can also question whether the use of QKD is necessary.

Several researchers have stated that the drawbacks of QKD networks shown in Table 5 may be solved with time. Reference [134] states that "more research is needed to develop a comprehensive security ecosystem". Reference [130] states that "the best that can be done at present is to integrate QKD with cryptographic schemes based on computational problems". Suppose it will take 20-30 years to fix the problems of QKD networks, to allow QKD networks to be deployed on a large-scale to millions/billions of users world-wide. The world then needs a temporary solution for today's cyber-security crisis, a solution that can last for the next 20-30 years, until QKD networks are ready to be deployed on a large scale. The SDD-WANs can provide a solution to today's cyber-security crisis, as they offer comparable security to QKD networks in practice, secured by the computational hardness of cracking SKC/PQC. The SDD-WANs also offer significant cost savings.

6. Experimental Results, European Union

Figure 3b illustrates SDD-WAN for the European Union, with 28 cities and 82 edges. Each city has a D-transceiver and a D-switch. Several SDD-WANs have been implemented on an Altera FPGA [43–45]. These hardware testbeds used a scheduling frame with 1,024 time-slots, and transmitted small packets with ≈ 20 bytes, at rates exceeding 400 million packets per second. The results of the hardware testbeds agreed exactly with the results of a Matlab software simulator, and all results agreed with theoretical expectations [42].

For this paper, the SDN control-plane programmed 744 D-flows into the EU topology, to achieve a very-high link utilization of 100% in sub-layer-3a. The EU network performance was determined using the software simulator.

In Figure 3b, let the fibers in sub-layer 3a support several optical channels operating at 800 Gbps, consistent with today's Silicon Photonics transceivers. Assume 1-Kbyte IP packets are used, and that an IP packet transmission requires 1 time-slot. (Larger IP packets can be fragmented into 1-Kbyte fragments, which are sent over sub-layer-3a.) Therefore, each time-slot has a duration of ≈ 10.24 nanoseconds, and a scheduling-frame (with F=1K) would have a duration of ≈ 10.5 microseconds.

Figure 5a illustrates the end-to-end queueing delays for several D-flows, in microseconds. The D-flows between London and Paris have queuing delays of about 1/3 of a microsecond. The D-flows between Stockholm and Madrid have queuing delays of about 1.5 microseconds. The end-to-end queueing delays are all ≤ 2 microseconds. Consider the D-flows between Stockholm and Madrid; the distance is ≈ 3,140 kilometers. Assuming a velocity of light in fiber of 200 km/millisecond, the fiber latency is ≈ 16 milliseconds. The queueing delay is ≈ 1,000 times smaller than the end-to-end fiber delay, which agrees with the theory presented in [42].

Figure 5b illustrates the end-to-end delay jitter of the packets, upon arrival at a D-transceiver. All packets experience a delay jitter ≤ 1 μsec. The jitters are a small fraction of the end-to-end fiber delays in the EU network, which are measured in 10s of milliseconds.

Figure 5c illustrates the evolution of the node Q-size (i.e.., the total number of packets queued per city) versus time, assuming an empty network at time-slot 0. (Results shown for selected cities.) The vertical lines represent the start of a new scheduling frame (with F=1,024 time-slots). The most heavily-loaded D-switch occurs at Berlin, with a steady-state size of about 103 packets. According to Figure 5d, the most lightly-loaded D-switch occurs at Athens, with a steady-state size of about 15 packets. The Q-sizes reach steady-state relatively-constant values after ≈ 4 scheduling frames, or ≈ 4,096 time-slots.

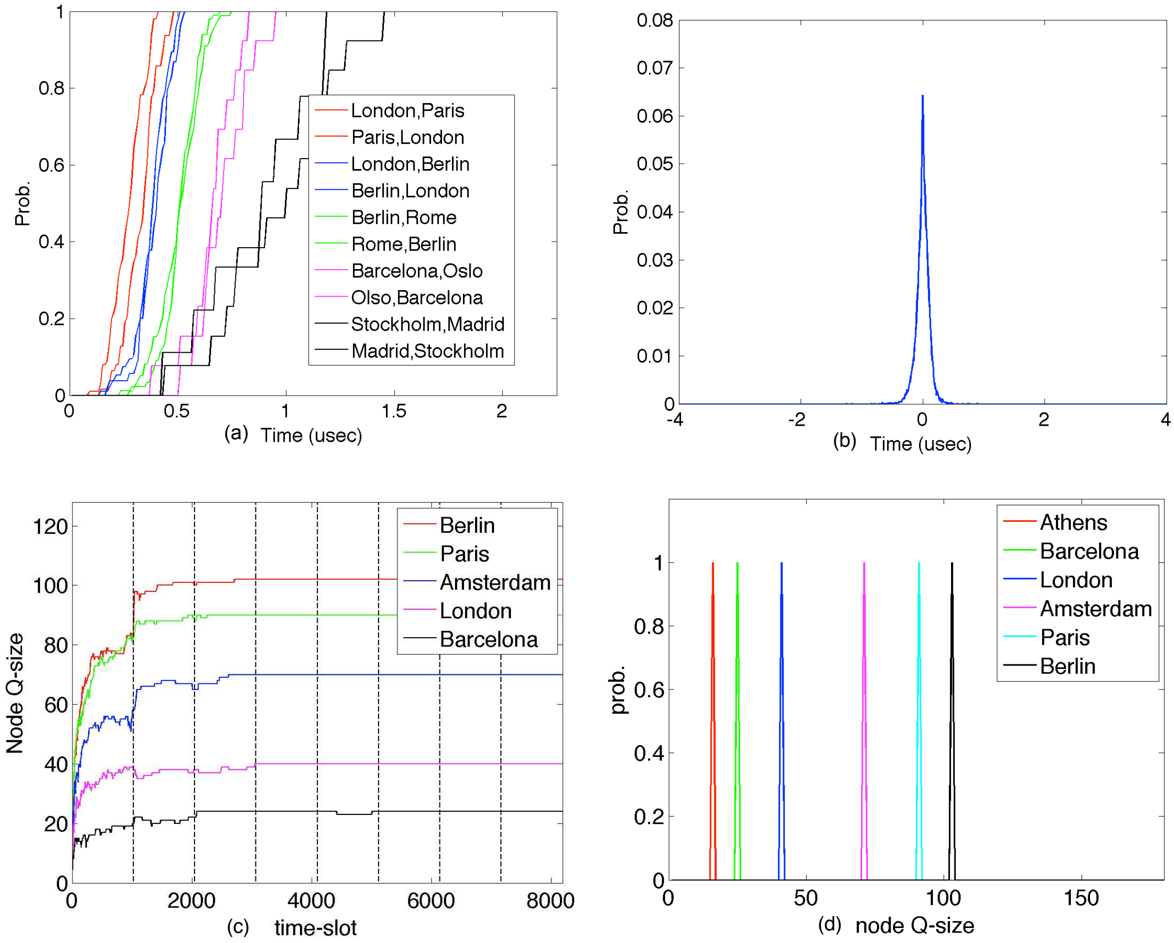


Figure 5. Performance of SDD-WAN for the European Union.

6.0.1. The BDP Buffer-Sizing Rule for BE-IP Routers

According to Figure 5d, the maximum Q-size is ≈ 105 packets, even when the links in sub-layer-3a operate at ≈ 100% utilization. Let the average "Round-Trip-Time" (RTT) of traffic in layer-3 equal 250 milliseconds. Assume a link of capacity C = 800 Gbps. The BDP rule-of-thumb states that the worst-case buffer size for the BE-IP link, to avoid exhausting a buffer, is $RTT \cdot C$, i.e., ≈ 25 Gigabytes for this example. Assuming 1-Kbyte packets, the worst-case buffer size needed for an 800 Gbps optical link is ≈ 25 million packets. A BE-IP router with degree 4 would require worst-case buffer sizes of ≈ 100 million packets. This rule-of-thumb illustrates the phenomena called "BufferBloat", where a layer-3 BE-IP router may buffer millions of packets for BE-flows [7]. As shown in Figure 6d, the use of D-switches has reduced the worst-case buffer size from potentially 100 million packets down to ≈ 105 packets, a reduction of ≈ 1,000,000 times.

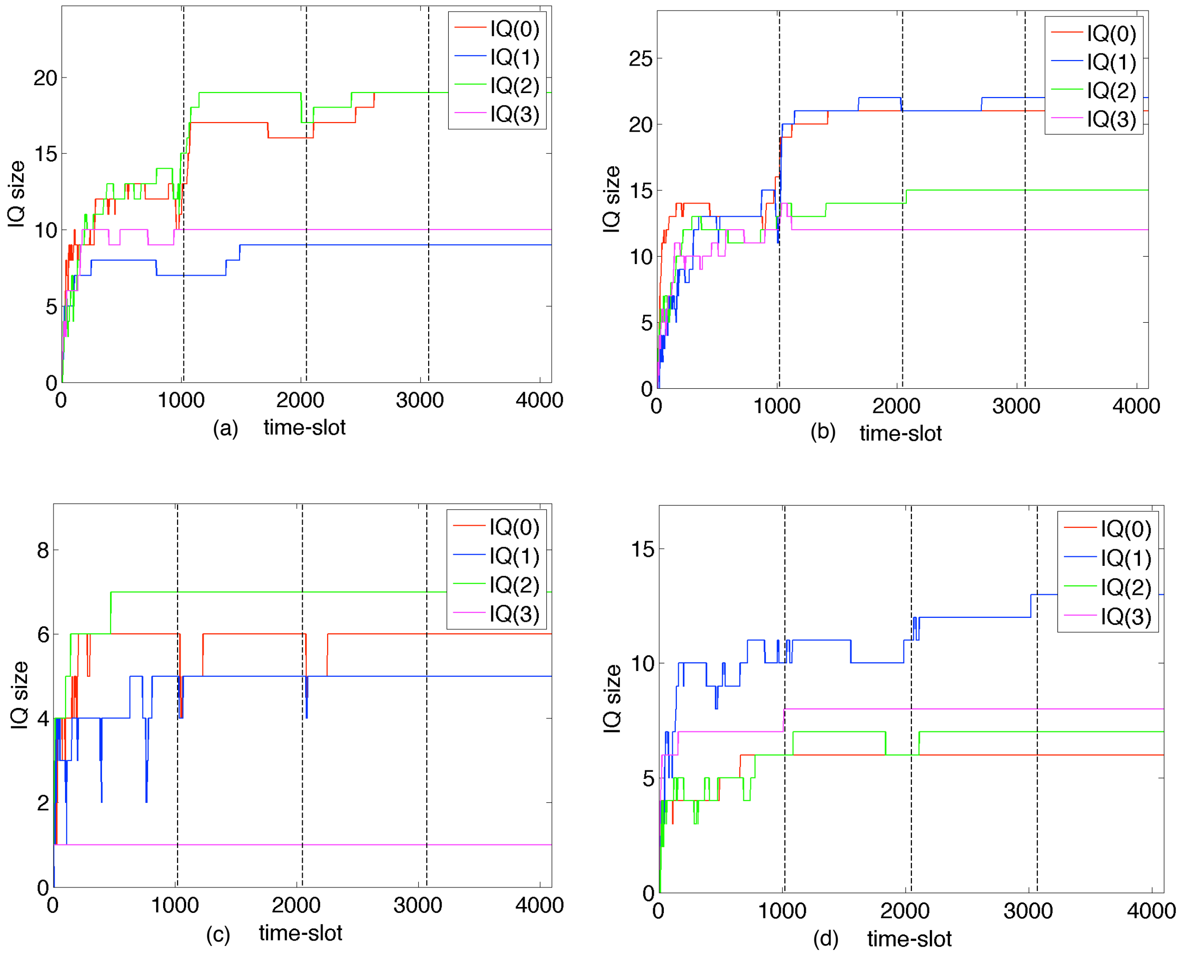


Figure 6. Evolution of IQs for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome).

6.0.2. The Small Buffer-Sizing Rule for BE-IP routers

Reference [95] presented a "Small-Buffer" rule-of-thumb, where the worst-case buffer size for each IoT link is $RTT \cdot C/\sqrt{N}$, where N is the number of long-lived TCP flows traversing a link. Letting $N \approx 1,024$, the Small-Buffer rule yields a worst-case buffer size of about 195K packets, a significant reduction. When compared to the "Small Buffer" rule, the use of D-switches can reduce the buffer size for a BE-IP router of degree 4 from $\approx$ 780K packets down to $\approx$ 105 packets, a reduction of $\approx$ 7,400 times.

6.0.3. A Deterministic Buffer-Sizing Rule for D-switches

For deterministic traffic, a new buffer-sizing rule can be stated (as first proposed in [41]). A "Deterministic Buffer Size" rule states that the amount of buffering required in a D-switch, to achieve 100% throughput and avoid exhausting a buffer, is K packet buffers per D-flow, where K is a small integer that depends upon the "Smoothness" in the service that a D-flow receives [42], [121]. According to prior research [42],[121], the parameter K is $\approx 1/2$ packet per D-flow when very smooth low-jitter schedules are used. The "Smoothness" of a D-flow can be defined using "Network-Calculus", as the worst-case deviation (i.e., service lead or service lag) in the service the D-flow receives, relative to a perfectly-scheduled D-flow. The smoothness is called the "Normalized Service Lead/Lag" in [42][121].

Figure 6 illustrates the evolution of the size of the Input Queues (IQs) in 4 different D-switches in the EU network, versus time. The horizontal axis illustrates 4 scheduling frames, each with 1024 time-slots. The number of packets arriving to each IQ per time-slot is initially 0, and quickly increases during the first scheduling frame. By the 4th scheduling frame, the number of packets arriving to each

IQ per time-slot is has reached a steady-state value, and remains constant. These graphs illustrate the deterministic behaviour of the IQs in the D-switches. After about 4 scheduling-frames, a steady-state is reached, wherein the number of packets arriving at each IQ in time-slot f (for $1 \leq f \leq 1024$) remains constant, in each scheduling-frame.

As stated in the Security Properties (section 5), malicious packets from an external cyberattacker (that are transmitted when no transmissions have been scheduled) will break the deterministic pattern in Figure 6. They will violate a D-schedule, and will be immediately detected by the Guaranteed-IDS. Similar deterministic patterns are observed in Figures 7 and 8.

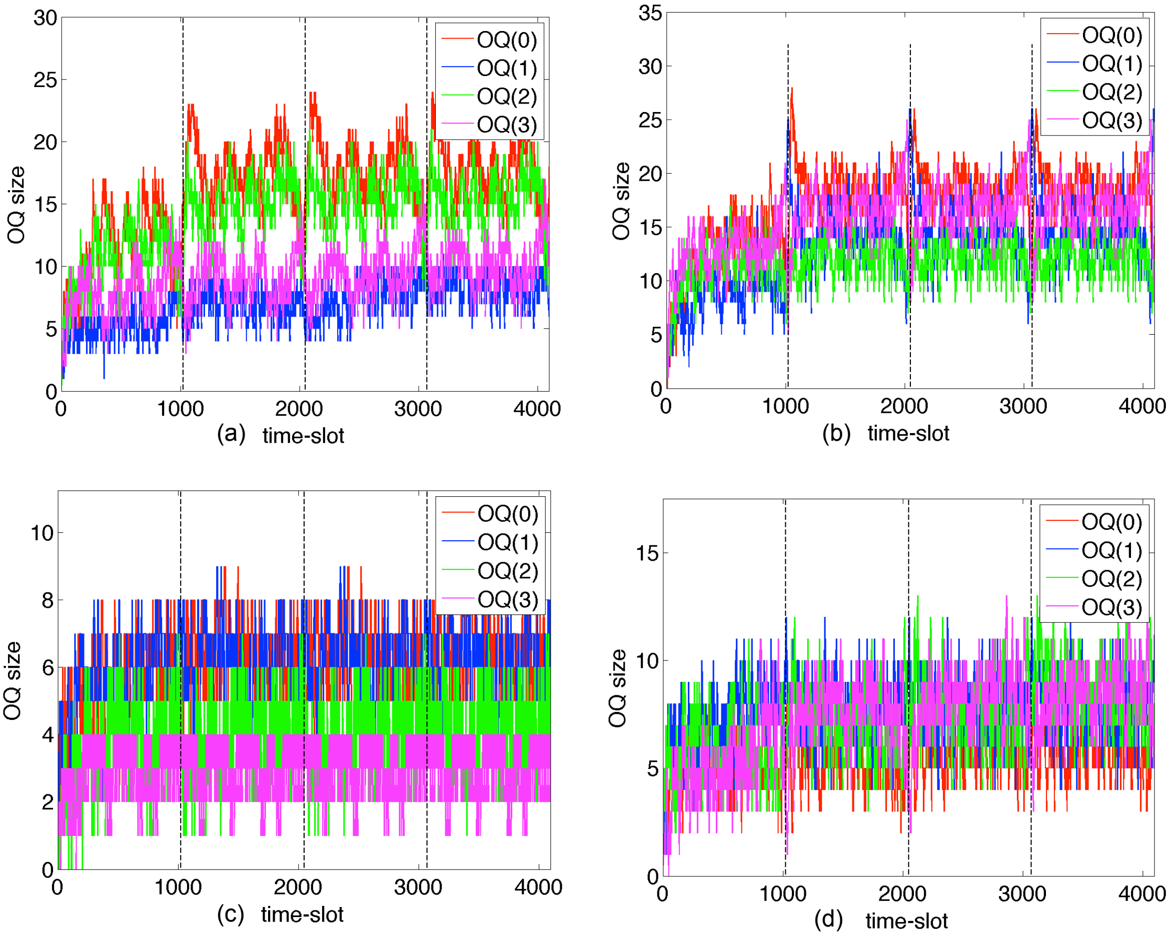


Figure 7. Evolution of OQs for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome).

Figure 7 illustrates the evolution of the size of the Output Queues (OQs) in 4 different D-switches in the EU network, versus time. The number of packets arriving to each OQ per time-slot is initially 0, and quickly increases during the first scheduling frame. These graphs illustrate the deterministic behaviour of the D-switches. After about 4 scheduling-frames, a steady-state is reached, wherein the number of packets arriving at each OQ in time-slot f (for $1 \leq f \leq 1024$) remains constant, in each scheduling-frame. This deterministic behaviour helps to detect cyber-attackers.

Figure 8 illustrates the evolution of the size of the Virtual Output Queues (VOQs) in 4 different D-switches in the EU network, versus time. (Only a few VOQs are shown for each switch.) The number of packets arriving to each VOQ per time-slot is initially 0, and quickly increases during the first scheduling frame. These graphs illustrate the deterministic behaviour of the D-switches. After about 4 scheduling-frames, a steady-state is reached, wherein the number of packets arriving at each VOQ in time-slot f (for $1 \leq f \leq 1024$) remains constant, in each scheduling-frame. This deterministic behaviour helps to detect cyber-attackers.

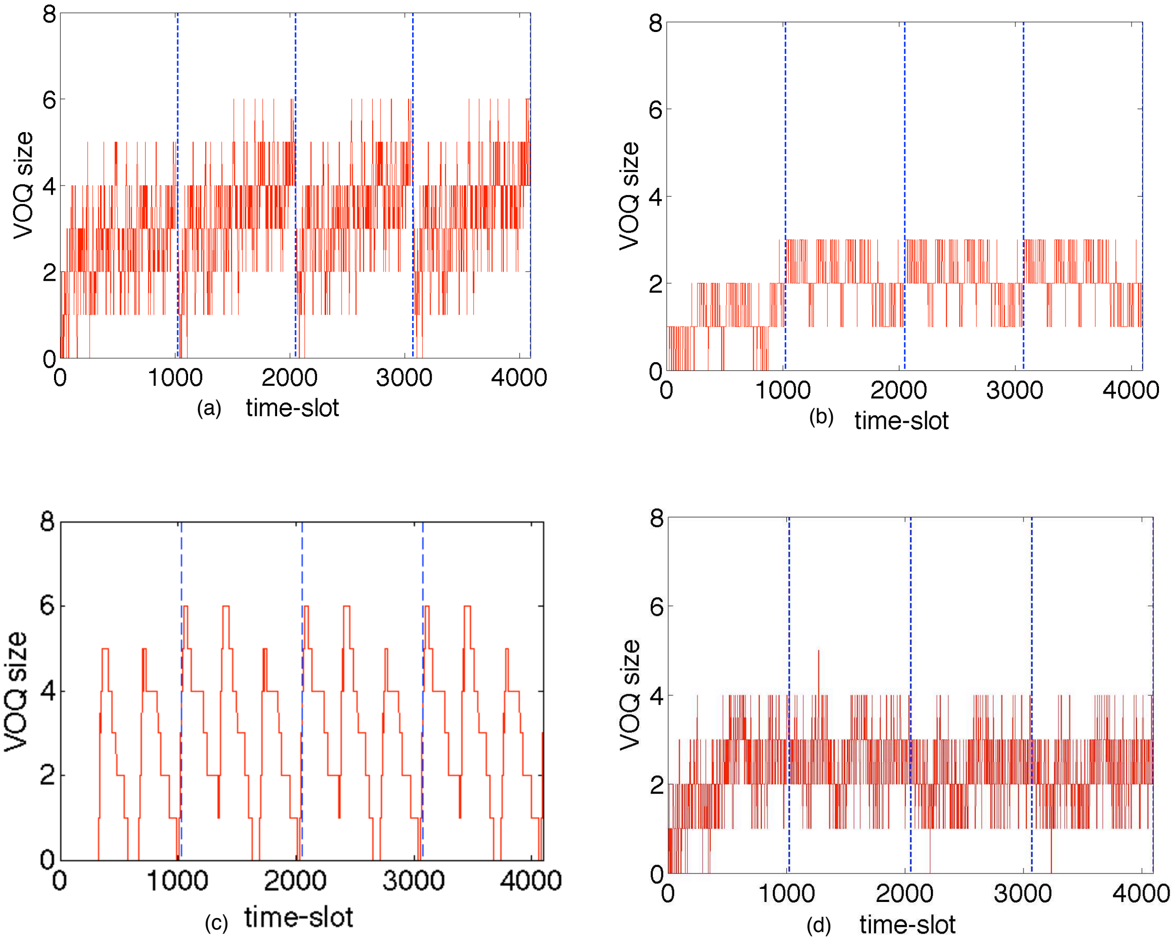


Figure 8. Evolution of VOQs for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome).

7. The Costs of the layer-3 BE-IP Network

Table 6 shows the 2022 annual revenues for many layer-3 equipment manufacturers in US dollars (please see their 2022 annual reports). (Alcatel/Lucent Technologies was purchased by Nokia in 2015). In 2022, Cisco reported revenues of US$51.6 billion. About 75% of this figure represents products, while about 25% represents services. In 2022, the total global revenue is ≈ US$180 Billion USD. Assuming 50% of the total represents the revenue for layer-3 equipment, then the global capital costs of layer-3 BE-IP equipment can be estimated at ≈ US$90 Billion in 2022.

Cisco estimates that about 95% of configuration changes in layer-3 equipment (i.e., routers and firewalls) are performed manually [10,11], and that the annual operational costs of layer-3 are about 2.5 times the annual capital costs. Hence, the global operational costs can be estimated at ≈ US$225 billion annually (in 2022). The combined global capital and operational costs for layer-3 are about US$315 billion annually in 2022.

According to Cisco, the global Internet carried about 9.1 billion Gigabytes of traffic per day in 2021, corresponding to an average global Internet traffic rate of 847 Tbps (Terabits per second) [10,11]. According to Google, layer-3 links operate at ≈ 25% utilization [100]. Hence, the global costs (capital and operational) due to "over-provisioning" can be estimated at 75% of the total global costs, i.e., US$236 billion annually in 2022. The use of SDD-WANs can improve the performance of the global Consumer-IoT network, by migrating traffic from the Best-Effort pillar to the Deterministic pillar shown in Figure 1b. The SDD-WAN in sub-layer-3a offers a much higher capacity with much lower delays, and much lower costs.

Table 6. Revenue from 2022 Annual Reports.

Company	2022 Annual Revenue (USD)
Arista	$4.381 Billion USD
Cisco	$51.6 Billion USD
Huawei	$92.380 Billion USD
Juniper	$5.301 Billion USD
Nokia	$26.251 Billion USD
Total	$179.91 Billion USD

Consider the SDD-WAN for the EU shown in Figure 2b with 28 cities, each with a D-switch. Let each D-switch uses 10 parallel Intel Stratix FPGAs, for a capacity of ≈ 35 Tbps. The cost of 280 FPGAs is ≈ US$2.1 million. Each FPGA requires some extra components (i.e., transducers (i.e., electrical-to-optical), D-transceivers, and power supplies), costing ≈ $150K. The total capital cost for the EU network is ≈ US$44 million, a relatively small value. The peak capacity is ≈ 980 Tbps, slightly larger than the average global Internet traffic rate of 847 Tbps (in 2021). The peak capacity of the SDD-WAN equals ≈ 10.5 billion Gigabytes of traffic per day.

Assuming 1 Kbyte packets, the FPGAs can transmit about 119 billion packets per second over the EU. Recall that the FPGAs implement "Guaranteed Intrusion Detection Systems" in hardware. The FPGAs can easily detect even a single un-authorized or malicious packet, sent from any type of external cyber-attacker, out of ≈ 119 billion transmitted packets/second. Equivalently, the FPGAs can can detect even a single un-authorized/malicious packet, embedded within ≈ 10.5 billion Gigabytes of traffic/day traversing the SDD-WAN. The SDD-WAN over the EU offers a vast capacity for a negligible cost, and provides exceptionally-strong hardware-enforced cyber-security.

The same technology can improve cyber-security for critical infrastructure, in smaller Regional Area, Metro Area and Local Area Networks. If twenty times as many FPGAs are introduced into the EU (i.e., 4480 FPGAs), then the peak capacity is ≈ 19,600 Tbps, and the capital cost is ≈ US$880 million (which is relatively small, compared to global capital and operational costs of layer-3).

According to Cisco, the majority of layer-3 traffic in the Consumer-IoT was IP-video in 2021 (about 82%). Let the IP-video traffic be migrated to the SDD-WAN in the Deterministic pillar in Figure 1b, and transported by D-flows. This migration can lower the capital and operational costs of the layer-3 Consumer-IoT by ≈ 82% each. The global cost savings can reach 82% of the combined global capital and operational costs of ≈ US$315 billion annually, equalling a savings of about US$260 billion annually. It is safe to say that the cost savings are in the range US$100s of billion annually.

7.1. MPLS-like Flow-Labels in Sub-layer 3a

The layer-3 BE-IP network includes many "Multi Protocol Label Switching" (MPLS) WANs. An MPLS-WAN consists of an MPLS control-plane, and a forwarding-plane of many MPLS packet-switches, similar to Figure 3a. Each MPLS packet includes a "flow-label" in its header, to identify the traffic flow. Each MPLS-switch maintains a "flow-table", that stores several values associated with each D-flow, i.e., the desired output port. The D-switches can be modified to perform some simple packet header processing in sub-layer-3a. The D-switches can still retain a dramatic simplification compared to a layer-3 BE-IP router, as they do not perform complex layer-3 routing and scheduling algorithms. The routing and scheduling is still performed in the SDN control-plane.

For example, packets in a D-flow can use "flow-labels" to identify the D-flow. Flow-labels typically have about 20-24 bits (MPLS flow-labels have 24 bits, and IPv6 flow-labels have 20 bits). Each input port in a D-switch can have a high-speed "flow-table", with an entry for each possible flow-label. When a packet arrives at an input port, its flow-label is used to access a row of the flow-table. The row yields the desired output port for the packet, and a new flow-label to be used for the outgoing packet. The

SDN control-plane maintains the flow-tables in each D-switch. This approach offers three advantages: (a) it keeps the complex layer-3 routing and scheduling algorithms in the SDN control-plane, so that D-switches remain simple and secure; (b) it eliminates the need to loosely-synchronize D-switches in sub-layer-3a, as each packet will now carry a flow-label in its header to be used in a lookup-table in each D-switch; (c) it retains the security features of the proposed SDD-IIoT (as every packet in a D-VPN must still pass the "Authorization Check" at a D-transceiver).

8. Conclusions

The Consumer-IoT has relied upon "Best-Effort" communications for 4 decades. It provides no guarantees that data is delivered by a deadline, or delivered at all. It is vulnerable to congestion and BufferBloat, and numerous layer-3 cyber-attacks. The Consumer-IoT will suffer from $\approx$ 17.5 million DoS/DDoS attacks in 2024, and $\approx$ 20 million attacks in 2025. Achieving cyber-security in the Internet is a "Grand-Challenge" problem for the 21st century [19], and the world needs new ideas for the cyber-security crisis.

This paper has explored exceptionally-strong hardware-enforced cyber-security in a next-generation "Software-Defined Deterministic Industrial Internet of Things" (SDD-IIoT). The SDD-IIoT introduces a new forwarding-plane (i.e., sub-layer-3a) for programmable deterministic M2M traffic flows (D-flows), comprising many simple authenticated D-switches, implemented with FPGAs. The forwarding-plane can support many SDD-WANs, which utilize an "Admission-Control/Access-Control" system, to control access to network bandwidth. The AC/AC system utilizes many collaborative AI rule-based "Zero Trust Architectures". The ZTAs and FPGAs implement hardware-enforced "Guaranteed Intrusion Detection Systems", which can process billions of Gigabytes of Internet traffic per day, to detect all external cyber-attacks in real-time and in hardware.

The traditional "Narrow-Waist" model of the Consumer-IoT was proposed three decades ago. To illustrate the next-generation IoT graphically, a "dual-pillar" service model is proposed, with a Best-Effort pillar to support the Consumer-IoT, and a Deterministic pillar to support the Industrial-IoT. The Deterministic pillar includes an AC/AC system to control access to network bandwidth. It implements "Authenticated Encrypted Deterministic Channels" in hardware in sublayer-3a, to support M2M traffic.

The SDD-IIoT offers several benefits:

- (1) Fine-grain access-control to network bandwidth will eliminate all congestion, BufferBloat, and DoS/ DDoS attacks in sublayer-3a, reduce buffer-sizes by 100,000-1,000,000 times, and reduce end-to-end delays to the speed-of-light in fiber.
- (2) Each nation can significantly strengthen its national security, by reducing the annual number of external cyber-attacks against its critical infrastructure to zero, secured by the computational hardness of cracking SKC/PQC. With a sufficiently-strong knowledge-base, each nation can also reduce or eliminate the number of internal cyber-attacks against its critical infrastructure. This benefit can have geo-political implications, i.e., Ukraine, Iran and Israel could achieve immunity to external cyber-attacks, relatively quickly.
- (3) It innovates the layer-3 infrastructure, to include a Deterministic Pillar of communications, and a forwarding-plane for M2M traffic flows, using low-cost FPGAs. Network operators can save US$100s of billions per year in reduced capital, energy and operational costs;
- (4) It can can reduce the global costs of cybercrime to society, estimated to exceed US$10 trillion per year in 2025.
- (5) It can support the Metaverse, by providing large increases in layer-3 capacity and security, while decreasing capital costs by US$100s of billions per year.
- (6) It can enable QKD networks, by providing "authenticated classical channels" in programmable layer-3 network which is immune to external cyber-attacks. Such channels are needed for the control QKD networks and the future Quantum Internet. Given a sufficiently-strong knowledge-base for the ZTAs, the number of internal cyber-attacks can also be significantly-reduced or eliminated.

- (7) According to the US "National Security Agency", QKD Networks cannot authenticate the source, and are vulnerable to insider attacks and DoS attacks. The solutions typically require the use of SKC/PQC, which lowers the security of QKD to the computational hardness of cracking SKC/PQC. As a result, the US NSA does not recommend QKD networks. In practice, the SDD-WANs can have comparable security to QKD networks, determined by the computational hardness of cracking SKC/PKC. The SDD-WANs can thus provide a solution to today's cyber-security crisis, until that time when QKD networks are ready to be deployed on a large-scale to millions/billions of user world-wide.

Funding: This research was performed as part of Prof. Szymanski's consulting practice, and was funded through his consulting practice.

Data Availability Statement: A large amount of data (i.e., graphs and their interpretations) is available in the author's prior publications and US patents, which are cited in the text.

Conflicts of Interest: The author is the owner of several US patents on deterministic networks that are referenced in this paper.

Appendix A

Table A1. Commonly used Acronyms.

Acronym	Description
AE	US NIST and IETF "Authenticated Encryption" algorithm
AEDC	"Authenticated and Encrypted Deterministic Channel" (i.e., a D-flow)
AES	US NIST "Advanced Encryption Standard" cipher
BE	"Best-Effort"
BE-IP, BE-flow	Best-Effort Internet Protocol, Best-Effort traffic flow
BE-VPN	a layer-3 BE "Virtual Private Network" (in the Consumer-IoT)
BGP	"Border Gateway Routing Protocol", to route packets in the C-IoT
BSD	"Berkeley Sockets Distribution" software, to program "sockets" in the C-IoT
C-IoT	Consumer-IoT
D, D-flow,	"Deterministic", i.e., a "deterministic traffic flow" (i.e., AEDC)
D-switch, D-IIoT	deterministic packet switch, Deterministic Industrial-IoT
D-schedule	a '"fine-grain" deterministic periodic schedule, to control a D-switch
DetNet Converged-WAN	the IETF DetNet Converged-WAN network (see IETF DetNet documents)
D-VPN	a layer-3 "Deterministic Virtual Private Network", (in the D-IIoT)
ETSI	European Telecommunications Standards Institute
IETF	Internet Engineering Task Force
ICMP, IGP	Internet Control Message Protocol, Interior Gateway Protocol
IDS, IDPS	Intrusion Detection System, Intrusion Detection and Prevention System
IKEV1, IKEV2	IETF Internet Key Exchange, version 1 and version 2
NIST	US National Institute for Standards in Technology
NSA	US National Security Agency
PKC, PKI	Public Key Cryptography, Public Key Infrastructure
PSK	Pre-Shared (secret) Key
PQC	Post Quantum Cryptography
SDN	Software Defined Networking
SDD-WAN	Software Defined Deterministic Wide Area Network
SDD-IIoT	Software Defined Deterministic Industrial Internet of Things
SKC	Symmetric Key Cryptography
TLS	Transport Layer Security (see IETF RFC 8446, Aug. 2018)
ULL	Ultra-Low Latency
ZTA	Zero Trust Architecture

Table A1 briefly summarizes the most common acronyms used in this paper. Table A2 briefly summarizes the common cyber-attacks in the Consumer-IoT.

Table A2. Common Cyber-attacks in the Consumer-IoT.

Threat/Attack Name	Type of Threat/Attack in Consumer-IoT	Type of Threat/Attack in SDD-IIoT
DoS/DDoS Attack	overload server(s) with many malicious IP traffic flows from many compromised devices	—- Effectively Eliminated —- SDD-IIoT does not use IP (or IP packet headers)
Spoofing attack	Modify IP packet headers to masquerade as a trusted peer	—- Effectively Eliminated —— SDD-IIoT does not use IP (or IP packet headers)
Phishing attack	Provide malicious email or link to malicious website	—- Effectively Eliminated—- links to malicious websites will not be pre-approved
Spear Phishing attacks	personalized contact to individual. Provide malicious email or link to malicious website	—- Effectively Eliminated—- links to malicious websites will not be pre-approved
Man in the Middle (MITM) attack	cyberattacker is interposed between two communicating entities by spoofing	—- Effectively Eliminated —— spoofing attacks eliminated (IP is not used)
Replay attack	a valid encrypted packet is observed and recorded, and re-introduced at a later time, as a malicious packet	—- Effectively Eliminated —— Authorization-Check detects all malicious packets
Reconnaissance attack (Harvest Now, Decrypt Later attack)	eavesdropping on encrypted TLS flows	—- Effectively Eliminated —- by Quantum-Safe ciphers
Malware attack (Remote Code Execution attack) (Application Vulnerability attack) (Cross Site Scripting attack) (Ransomware attack)	vulnerable host-computer can render control to cyber-attacker under special circumstances (i.e., Java remote code execution)	—- Effectively Eliminated — links to malicious websites will not be pre-approved

References

1. Li Z, Uusitalo MA., Shariatmadari H, and Singh B., "5G URLLC: Design Challenges and System Concepts", Int. Symp. on Wireless Comm. Systems (ISWCS), Lisbon, Portugal, 2018 pp. 1-6.
2. Pokhrel SR., Ding J., Park J., Park OS., Choi J., "Towards Enabling Critical mMTC: A Review of URLLC within mMTC", IEEE Access, 2020, 8, pp. 131796-131813.
3. Park J., Samarakoon S., Shiri H., Abdel-Aziz MK., Nishio T., Elgabli A., Bennis M., "Extreme Ultra-Reliable and Low-Latency Communication", Nature Electronics, March 2022, 5(3), pp. 133-141.
4. Gevros P., Crowcroft J., Kirstein P., and Bhatti S., "Congestion Control Mechanisms and the Best Effort Service Model," IEEE Network, vol. 15, no. 3, May-June 2001, pp. 16-26.
5. Lefelhocz C., Lyles B., Shenker S., Zhang L., "Congestion Control for Best-Effort Service: Why we need a New Paradigm", IEEE Network, Jan. 1996, 10(1), pp.10-19.
6. Afanasyev A., Tilly N., Reiher P. and Kleinrock L., "Host-to-Host Congestion Control for TCP", IEEE Comm. Surveys and Tutorials, 3Q Vol. 12, No. 3, 2010, pp. 304-342.
7. Gettys J., Nichols K., "BufferBloat: Dark Buffers in the Internet", ACM Queue, Vol. 9, No. 11, Nov. 29, 2011, pp. 40-54.
8. Butler K., Farley TR., McDaniel P., and Rexford J., "A Survey of BGP Security Issues and Solutions", Proc. IEEE, 98(1), 2009, pp.100-122.
9. Goldberg S., "Why is it Taking So Long to Secure Internet Routing?", CACM, Vol. 57, No. 10, Oct. 2014, pp. 56-63.

10. CISCO, "Cisco Annual Internet Report (2018-2023)", Available online: https://cisco.com (Accessed on June 2023)
11. CISCO, "Global - 2021 Forecast Highlights", Available online: https://www.cisco.com (Accessed on June 2023)
12. Kleinrock L., et al, "Realizing the Internet Future: The Internet and Beyond", National Research Council, National Academy Press, Washington DC, 1994
13. Popa L., Ghodsi A., Stoica I., "HTTP as the Narrow Waist of the Future Internet", Proc. 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Oct. 20, 2010, pp. 1-6.
14. Akhshabi S, Dovrolis C., "The Evolution of Layered Protocol Stacks leads to an Hourglass-Shaped Architecture", Proc. ACM SIGCOMM Conf., Aug. 2011, pp. 206-217.
15. Beck M., "On the Hourglass Model", Comm. of the ACM., June 2019, 62(7), pp. 48-57.
16. Sisinni E., Saifullah A., Han S., Jennehag U., and Gidlund M., "Industrial Internet of Things: Challenges, Opportunities, and Directions", IEEE Trans. Industrial Informatics, 2018, 14(11), pp. 4724-4734.
17. US CISA (Cybersecurity and Infrastructure Security Agency), "Critical Infrastructure Security and Resilience", 2023.
18. NATO, "EU-NATO Task Force on the Resilience of Critical Infrastructure, Final Assessment Report", Available online, https://commission.europa.eu/system/files/2023, (Accessed on Nov. 2023)
19. US National Academy of Engineering, "NAE Grand challenges for engineering: Secure cyberspace". Available online: https://www.engineeringchallenges.org/challenges/cyberspace.aspx, (Accessed on June. 2023)
20. Wang LJ., Zhang KY., Wang JY. , et al, "Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography", npj Quantum Information, 2021, 7(1),67.
21. Douligeris C. and Mitrokotsa A., "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art", Computer Networks, 2004, 44(5), pp.643-666.
22. Yan Q., Yu FR., "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing", IEEE Comm. Mag., Apr. 2015, 53(4), pp. 52-59.
23. Somani, G. Gaur MS., Sanghi D., Conti M., Buyya R., "DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", Computer Communications, July 2017, 107, pp. 30-48.
24. Zlomislić V., Fertalj K., Sruk V., "Denial of Service Attacks, Defences and Research Challenges", Cluster Computing, Mar. 2017, 20, pp. 661-71.
25. Bawany N.Z., Shamsi J.A. and Salah K., "DDoS Attack Detection and Mitigation using SDN: Methods, Practices, and Solutions", Arabian Journal for Science and Engineering, 2017, 42, pp.425-441.
26. Praseed A., Thilagam PS., "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications", IEEE Comm. Surveys & Tutorials, Sept. 2018, 21(1), pp. 661-685.
27. Osterweil E., Stavrou A., Zhang L., "21 Years of Distributed Denial-of-Service: A Call to Action", IEEE Computer, Aug. 2020, 53(08), pp. 94-99.
28. Vishwakarma R. and Jain A.K., "A Survey of DDoS Attacking Techniques and Defence Mechanisms in the IoT Network", Telecommunication Systems, 2020, 73(1), pp.3-25.
29. Eliyan LF., Di Pietro R., "DoS and DDoS Attacks in Software Defined Networks: A Survey of Existing Solutions and Research Challenges", Future Generation Computer Systems, Sept. 2021, 122, pp. 149-171.
30. Rescorla E., IETF RFC 8446, "The Transport Layer Security (TLS) Protocol Version 1.3", Aug. 2018, pp. 1-160.
31. Jager T., Kohlar F., Schäge S. and Schwenk J., “On the Security of TLS-DHE in the Standard Model” In Advances in Cryptology–CRYPTO 2012: 32nd Annual Cryptology Conf., Santa Barbara, CA, USA, August 19-23, 2012, Springer Berlin Heidelberg, pp. 273-293.
32. Krawczyk H., Paterson K.G. and Wee,H., 2013, August. “On the Security of the TLS Protocol: A Systematic Analysis”, Annual Cryptology Conf., Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 429-448.
33. Bhargavan K., Fournet C., Kohlweiss M., Pironti A. and Strub P.Y., “Implementing TLS with Verified Cryptographic Security”, In 2013 IEEE Symp. on Security and Privacy, May 2013, pp. 445-459.
34. Bürstinghaus-Steinbach K., Krauß C., Niederhagen R. and Schneider,M., “Post-quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and Sphincs+ with mbed tTLS”, Proc. 15th ACM Asia Conf. on Computer and Comm. Security, Oct. 2020, pp. 841-852.

35. Eldewahi AE., Sharfi TM., Mansor AA., Mohamed NA., Alwahbani SM., "SSL/TLS Attacks: Analysis and Evaluation", IEEE Int. Conf. on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), Sept. 2015, pp. 203-208.
36. Sirohi P., Agarwal A., Tyagi S., "A Comprehensive Study on Security Attacks on SSL/TLS Protocol", IEEE Int. Conf. on Next Gen. Computing Technologies (NGCT), Oct. 2016, pp. 893-898.
37. Waked L., Mannan M., Youssef A., "The Sorry State of TLS Security in Enterprise Interception Appliances", Digital Threats: Research and Practice, May 2020, 1(2), pp. 1-26.
38. Paracha MT., Dubois DJ., Vallina-Rodriguez N., Choffnes D., " IoTLS: Understanding TLS Usage in Consumer IoT Devices", Proc. 21st ACM Int. Measurement Conf, Nov. 2021, pp. 165-178.
39. Meyer C., Schwenk J., "SoK: Lessons Learned from SSL/TLS Attacks", Int. Workshop on Information Security Applications, Cham: Springer International Publishing, Aug. 2013, pp. 189-209.
40. Mell P, Marks D., McLarnon M., "A Denial-of-Service Resistant Intrusion Detection Architecture", Computer Networks, Oct. 2000, 34(4), pp. 641-658.
41. Szymanski TH., "The “Cyber Security via Determinism Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT)", IEEE Access, April 2022, 10, pp. 45893-45930,
42. Szymanski TH., "An Ultra Low Latency Guaranteed-Rate Internet for Cloud Services", IEEE Trans. on Networking, Feb. 2016 (posted online 2014), Vol. 24, No. 1, pp. 123-36.
43. Szymanski TH., "Supporting Consumer Services in a Deterministic Industrial Internet Core Network", IEEE Communications Magazine, June 2016, Vol. 54, No. 6, pp. 110-117.
44. Szymanski TH., "Securing the Industrial-Tactile Internet of Things with Deterministic Silicon Photonic Switches", IEEE Access, Sept. 2016, Vol. 4, pp. 8236-8249.
45. Szymanski TH., "Security and Privacy for a Green Internet of Things" IEEE IT Professional, Oct. 2017, Vol. 19, No. 5, pp. 34-41.
46. Tehranipoor M., Wang C., editors, "Introduction to Hardware Security and Trust", Springer Science & Business Media, Sept. 2011.
47. Maistri P., "Countermeasures against Fault Attacks: The Good, the Bad, and the Ugly", IEEE 17th Int. On-Line Testing Symp., July 2011, pp. 134-137.
48. Jin Y., "Introduction to Hardware Security", Electronics, Oct. 2015, 4(4), pp. 763-784.
49. Alioto M., "Trends in Hardware Security: From Basics to ASICs", IEEE Solid-State Circuits Magazine, Aug. 2019, 11(3), pp. 56-74.
50. Nir Y. and Langley A., "Chacha20 and Poly1305 for IETF Protocols", IETF RFC 7539, May 2015, pp. 1-45.
51. Nasrallah A., Thyagaturu AS., Alharbi Z., Wang C., Shao X., Reisslein M., ElBakoury H., "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research", IEEE Comm. Surveys and Tutorials, Sept. 2018, 21(1), pp. 88-145.
52. Butun I., Osterberg P., Song H., "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures", IEEE Comm. Surveys & Tutorials, Nov. 2019, Vol. 22, No. 1, pp. 616-44.
53. Khan MA., and Salah K., "IoT Security: Review, Blockchain Solutions, and Open Challenges", Elsevier, Future Generation Computer Systems, 2018, Vol. 82, pp. 395-411.
54. Hassija V., Chamola V., Saxena V., Jain D., Goyal P., and Sikdar B., "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures." IEEE Access, 2019, Vol. 7, pp. 82721-82743.
55. Neshenko N., Bou-Harb E., Crichigno J., Kaddoum G., and Ghani N., "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations." IEEE Comm. Surveys & Tutorials, 2019, Vol. 21, No. 3, pp. 2702-2733.
56. Karie NM., Sahri NM., ang W., Valli C., and Kebande VR., "A Review of Security Standards and Frameworks for IoT-Based Smart Environments", IEEE Access, Sept. 2021, Vol. 9, pp. 121975-121995.
57. Xin Y., Kong L., Chen Y., Li Y., Zhu H., Gao M., Hou H., and Wang C., "Machine Learning and Deep Learning Methods for Cybersecurity", IEEE Access, 2018, Vol. 6, pp. 35365-35381.
58. Al-Garadi MA., Mohamed A., Al-Ali AK., Du X., Ali I., and Guizani M., "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security", IEEE Comm. Surveys & Tutorials, 2020, Vol. 22, No. 3, pp. 1646-1685.
59. Hussain F., Hussain R., Hassan SA., and Hossain E., "Machine Learning in IoT Security: Current Solutions and Future Challenges", IEEE Communications Surveys & Tutorials, 2020, Vol. 22, No. 3, pp. 1686-1721.

60. Demertzi V., Demertzis S., Demertzis K., "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities" Applied Sciences, Jan. 2023, 13(2), pp. 790.
61. de Azambuja AJ., Plesker C., Schützer K., Anderl R., Schleich B., Almeida VR., "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey", Electronics, Apr. 2023, 12(8). pp. 1920.
62. Sandhu R., Ferraiolo D., Kuhn R., ”The NIST Model for Role-Based Access Control: Towards a Unified Standard”, ACM workshop on Role-Based Access Control, July 2000, Vol. 10, No. 344287.344301.
63. Kuhn DR., Coyne EJ., Weil TR., “Adding Attributes to Role-Based Access Control”, IEEE Computer, June 2010, Vol. 43, No. 6, pp. 79-81.
64. Hu VC., Ferraiolo D., Kuhn R., Friedman AR., et al, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)”, NIST Special Publication 800-162, April 2013, pg. 1-54.
65. Hu VC., Kuhn DR., Ferraiolo DF., Voas J., “Attribute-Based Access Control”, IEEE Computer, Vol. 16, No. 48(2), pp. 85-88, Feb. 2015.
66. The White House, "Executive Order on Improving the Nation’s Cybersecurity", May 12, 2021.
67. US NIST (National Institute for Standards and Technology), "Zero Trust Architecture", Publication SP-800-207, Aug. 2020. Available online: http://csrc.nist.gov/publications (Accessed June 2023).
68. Kerman A., Borchert O., Rose S., Tan A., "Implementing a Zero Trust Architecture", The MITRE Corporation, Tech. Rep., Oct. 2020.
69. Bace R., Mell P., “NIST Special Publication on Intrusion Detection Systems”, Nov 1. 2001, Available online: https://www.nist.gov/publications (Accessed June 2023).
70. Scarfone K., Mell P., “Guide to Intrusion Detection and Prevention Systems (IDPS)”, NIST Special Publication 800-94, , Feb. 2007, pp. 1-127, Available online https://www.nist.gov/publications (Accessed June 2023).
71. Mukherjee B., Heberlein TD., Levitt KN., "Network Intrusion Detection." IEEE Network, 1994, 8, No. 3, pp. 26-41.
72. Debar H., Dacier M., Wespi A., “Towards a Taxonomy of Intrusion-Detection Systems”, Elsevier Computer Networks, April 1999, Vol. 31, No. 8, pp. 805-822.
73. Hubballi N., and Suryanarayanan V., "False Alarm Minimization Techniques in Signature-Based Intrusion Detection Systems: A Survey", Computer Communications, 2014, Vol. 49, pp. 1-17.
74. Masdari M., and Khezri H., "A Survey and Taxonomy of the Fuzzy Signature-based Intrusion Detection Systems", Applied Soft Computing, 2020, Vol. 92, pp. 106301.
75. Garcia-Teodoro P., Diaz-Verdejo J., Macia-Fernandez G., and Vazquez E., "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges", Computers & Security, 2009, 28, No. 1-2, pp. 18-28.
76. Jyothsna V., Prasad R., and Prasad KM., "A Review of Anomaly Based Intrusion Detection Systems", Int. Journal of Computer Applications, 2011, Vol. 28, No. 7, pp. 26-35.
77. Javaid A., Niyaz Q., Sun W., and Alam M., "A Deep Learning Approach for Network Intrusion Detection System", Eai Endorsed Trans. on Security and Safety, 2016, Vol. 3, No. 9, e2.
78. Yin C., Zhu Y., Fei J., and He X., "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks", IEEE Access, 2017, Vol. 5, pp. 21954-21961.
79. Shone N., Ngoc TN., Phai VD., and Shi Q., "A Deep Learning Approach to Network Intrusion Detection" , IEEE Trans. on Emerging Topics in Comp. Intelligence, Feb. 2018, Vol. 2, No. 1, pp. 41-50.
80. Vinayakumar R., Alazab M., Soman KP., Poornachandran P., Al-Nemrat A., and Venkatraman S., "Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Access, 2019, Vol. 7, pp. 41525-41550.
81. US NIST (National Institute of Standards and Technology), Federal Information Processing Standards (FIPS), Publication 197, "Announcing the Advanced Encryption Standard (AES)", 2001. Available online: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines, Accessed June 2022.
82. Daemen J. and Rijmen V., "The Design of Rijndael", New York: Springer-verlag, March 2002.
83. McGrew D., “An Interface and Algorithms for Authenticated Encryption”, IETF, RFC 5116, Jan. 2008.
84. Bozhko AA., “Properties of AEAD Algorithms”, Draft-IRTF-CFRG-AEAD-02, Oct. 2023.
85. Perlner RA., Cooper DA., "Quantum Resistant Public Key Cryptography: A Survey", Proc. 8th Symp. on Identity and Trust on the Internet, April 2009, pp. 85-93.
86. US NSA (National Security Agency), “Quantum Computing and Post Quantum Cryptography, FAQs (Frequently Asked Questions)”, Document PP-21-1120, Aug. 4, 2021, Available online: media.defense.gov/2021/Aug/04, Accessed April 2022.

87. Chen L., Jordan S., Liu YK., Moody D., Peralta R., Perlner R., Smith-Tone D., “Report on Post-Quantum Cryptography”, Vol. 12, US NIST Interagency/Internal Report (NISTIR) - 8105, April 2016, 10 pages. Available online: nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf
88. ETSI (European Telecommunications Standards Institute), Technical Report, "Quantum Safe Public Key Encryption and Key Encapsulation", ETSI TR 103 823 v1.1.2, Oct. 2021, Available online: www.etsi.org/standards-search, Accessed Jan. 2023.
89. ETSI (European Telecommunications Standards Institute), Technical Report, "Quantum Safe Virtual Private Networks", ETSI TR 103 617 v1.1.1, Aug. 2018, Available online: www.etsi.org/standards-search, Accessed Jan. 2023.
90. Xiao X., and Ni LM., "Internet QoS: A Big Picture", IEEE Network, 1999, Vol. 13, No. 2, pp. 8-18.
91. Nong G., and Hamdi M., "On the Provision of Quality-of-Service Guarantees for Input Queued Switches." IEEE Communications Mag., 2000, Vol. 38, no. 12, pp. 62-69.
92. Meddeb A., "Internet QoS: Pieces of the Puzzle." IEEE Communications Mag., 2010, Vol. 48, No. 1, pp. 86-94.
93. Parekh AK., and Gallager RG., "A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: the Single-Node Case", IEEE/ACM Trans. on Networking, 1993, Vol. 1, No. 3, pp. 344-357.
94. Parekh AK., and Gallager RG., "A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: the Multiple Node Case", IEEE/ACM Trans. on Networking, 1994, Vol. 2, No. 2, pp. 137-150.
95. Appenzeller G., Keslassy I., McKeown N., "Sizing Router b=Buffers", ACM SIGCOMM Computer Comm. Review 34,2004, No. 4, pp. 281-292.
96. Iyer S., Kompella RR., Mckeown N., "Designing Packet Buffers for Router Linecards", IEEE Trans. Networking, June 2008, Vol. 16, No. 3, pp. 705-717.
97. Anantharam V., McKeown N., Mekittikul A. and Walrand J., "Achieving 100% Throughput in an Input Queued Switch", IEEE Trans. Comm., 1999, Vol. 47, No. 8, pp. 1260-1267.
98. Mckeown N., "The iSLIP Scheduling Algorithm for Input-Queued Switches", IEEE/ACM Trans. on Networking, April 1999, Vol. 7, No. 2, pp. 188-201.
99. Odlyzko A., "Data Networks are Lightly Utilized, and Will Stay That Way", Review of Network Economics, 2003, 2, No. 3.
100. Hassidim A., Raz D., Segalov M., Shaqed A., "Network Utilization: The Flow View", IEEE Infocom, 2013, pp. 1429-1437.
101. Braken R., Clark D., Shenker S., "Integrated Services in the Internet Architecture - An Overview", IETF RFC 1633, July 1994.
102. Black D., Jones P., “Differentiated Services (DiffServ) and Real-Time Communications”, IETF RFC 7657, Nov. 2015.
103. IEEE 802.org, "Deterministic Ethernet: 802.1 Standards for Real-Time Process Control, Industrial Automation, and Vehicular Networks", 2012. Available online: www.ieee802.org (Accessed Nov. 2023).
104. Hermeto RT., Gallais A., Theoleyre F., "Scheduling for IEEE-802.15.4-TSCH and Slow Channel Hopping MAC in Low Power Industrial Wireless Networks: A Survey", Computer Communications, Dec. 2017, 1;114, pp. 84-105.
105. Dujovne D., Watteyne T., Vilajosana X., Thubert P., "6TiSCH: Deterministic IP-enabled Industrial Internet (of Things)", IEEE Comm. Mag, Dec. 2014, 52(12). pp. 36-41.
106. Finn N., Thubert P., "Deterministic Networking Problem Statement (04)", IETF Internet-Draft, Standards Track, Oct. 2015, pp. 1-17.
107. Grossman E., Gunther C., et al, "Deterministic Networking Use Cases", IETF draft, June 2018.
108. Finn N., Thubert P., Varga B., Farkas J., "Deterministic Networking Architecture", IETF Internet RFC 8655, Oct. 2019.
109. Liu B., Ren S., et al, "Towards Large-Scale Deterministic IP Networks", IEEE IFIP Networking Conf., June 2021, pp. 1-9.
110. Singla A., Chandrasekaran B. , Godfrey PB., Maggs B., "The Internet at the Speed of Light", ACM Hotnets 2014, LA, USA, Oct. 2014, pp. 1-7.
111. Fettweis G., Boche H., et al, "The Tactile Internet", ITU-T Technology Watch Report, Aug. 2014, pp. 1-24.

112. Chen WJ., Chang CS. , and Huang HY., "Birkoff-von Neumann Input Buffered Crossbar Switches for Guaranteed-Rate Services", IEEE Trans. Comm., July 2001, vol. 49, no. 7, pp. 1145-1147.
113. C.E. Koksal CE., R.G. Gallager RG. , and C.E. Rohrs CE., "Rate Quantization and Service Quality over Single Crossbar Switches", IEEE Infocom, 2004, Vol. 3, pp. 1962-1973.
114. Keslassy I., Kodialam M., Lakshman TV. and Stilliadis D., "On Guaranteed Smooth Scheduling for Input-Queued Switches", IEEE/ACM Trans. Networking, Dec. 2005, Vol. 13, No. 6, pp. 1364-1375.
115. Mohanty SR. , and Bhuyan LN., "Guaranteed Smooth Switch Scheduling with Low Complexity", IEEE Globecom, Nov. 2005, Vol. 1, pp. 5.
116. Chang CS., Lee DS., and Yue CY., "Providing Guaranteed Rate Services in the Load Balanced Birkhoff-von Neumann Switches", IEEE/ACM Trans. Networking, June 2008, Vol. 14. No. 3, pp. 644-656.
117. Szymanski TH., "A Low Jitter Guaranteed Rate Scheduling Algorithm for Packet Switched IP Routers", IEEE Trans. on Communications, Nov. 2009, Vol. 57, No. 11, pp. 3446-3459.
118. Szymanski TH., and D. Gilbert, "Internet multicasting of IPTV with essentially-zero delay jitter", IEEE Trans. Broadcasting, 55(1), pp.20-30, 2009.
119. Szymanski TH. and Gilbert D., "Provisioning Mission-Critical Telerobotic Control Systems over Internet backbone Networks with Essentially-Perfect QoS", IEEE Journal on Selected Areas in Comm., May 2010, Vol. 28, No. 5, pp. 630-643.
120. Szymanski TH., "Max-Flow Min-Cost Routing in a Future Internet with Improved QoS Guarantees", IEEE Trans. on Communications, April 2013, Vol. 61, No. 4, pp. 1485-1497.
121. Szymanski TH., "Method to Achieve Bounded Buffer Sizes and Quality of Service Guarantees in the Internet Network", US Patent 8,665,722 B2, March 2014.
122. Szymanski TH., "Method to Achieve Bounded Buffer Sizes and Quality of Service Guarantees in the Internet Network", US Patent 9,584,431 B2, Feb. 2017.
123. Szymanski TH., "Reduced-Complexity Integrated Guaranteed-Rate Optical Packet Switch", US Patent US 10,687,128 B2, June 2020.
124. Szymanski TH., "Methods to Strengthen Cyber-security and Privacy in a Deterministic Internet of Things", US Patent US 11,019,038 B2, May 2021.
125. Karakus M., Durresi A., "A Survey: Control Plane Scalability Issues and Approaches in Software-Defined Networking (SDN)", Computer Networks, Jan. 2017, Vol. 12, pp. 279-93.
126. Bannour F., Souihi S., Mellouk A., "Distributed SDN Control: Survey, Taxonomy, and Challenges", IEEE Comm. Surveys & Tutorials, Jan. 2018, Vol. 20, No. 1, pp. 333-54.
127. Diamanti E., Lo HK., Qi B., Yuan Z., "Practical Challenges in Quantum Key Distribution", npj Quantum Information, Nov. 2016, 2(1), pp. 1-12.
128. Cao Y., Zhao Y., Wang Q., Zhang J., Ng SX., Hanzo L., "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet", IEEE Comm. Surveys & Tutorials, Jan. 2022, 24(2), pp. 839-894.
129. Tsai CW., Yang CW., Lin J., Chang YC., Chang RS., "Quantum Key Distribution Networks: Challenges and Future Research Issues in Security" Applied Sciences, Apr. 2021, 11(9), pp. 3767.
130. Lella E., Schmid G., "On the Security of Quantum Key Distribution Networks", Cryptography, Oct. 2023, 7(4), 53.
131. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., Voznak M., "Quantum Key Distribution: A Networking Perspective", ACM Computing Surveys (CSUR), Sept. 2020, 53(5), pp. 1-41.
132. James P., Laschet S., Ramacher S., Torresetti L., "Key Management Systems for Large-Scale Quantum Key Distribution Networks", Proc.18th Int. Conf. on Availability, Reliability and Security, Aug. 2023, pp. 1-9.
133. ETSI GS QKD 004 2020, "Quantum Key Distribution (QKD); Application Interface, Group Specification v2.1.1", European Telecommunications Standards Institute (ETSI), Industry Specification Groups (ISG).
134. Green, A., Lawrence, J., Siopsis, G., Peters, N.A. and Passian, A., "Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams", Sensors, 2023, 23(24), p.9818.
135. Kaufman C., Hoffman P., Nir Y., Eronen P., "Internet Key Exchange Protocol Version 2 (IKEV2)", IETF RFC 5996, Sept. 2010, pp. 1-138.
136. Fluhrer S., Kampanakis P., McGrew D., Smyslov V., "Mixing Preshared Keys in IKEV2 for Post Quantum Security", IETF RFC 8774, Jan. 2020, pp. 1-20.

137. Bos JW., Costello C., Naehrig M., Stebila D., "Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning With Errors Problem", IEEE Symp. on Security and Privacy, May 2015, pp. 553-570.

Short Biography of Author

Ted H. Szymanski completed the PhD degree in ECE at the University of Toronto. From 1987-1998, he was at Columbia and McGill Universities. From 1999-2023, he was a professor in the ECE department at McMaster University. From 2001-2011, he held the "Bell Canada Chair in Data Communications at McMaster. From 1993-2003, he led the "Optical Architecture" project within a 10-year national research program, which demonstrated a free-space "intelligent optical backplane" using photonic packet-switches. Collaborators included Nortel Networks (now Ericsson), Newbridge Networks (now Alcatel), Lockheed-Martin/Sanders, and 4 universities (McMaster, McGill, U of T, and Heriot-Watt University, Edinburgh). He holds a US patent for the architecture, along with Dr. Scott Hinton, former head of Photonic Switching at Bell Labs.His research group also demonstrated the first photonic FPGA, fabricated through the US ARPA/Lucent/Coop foundry service. He holds 20 US patents, spanning the deterministic IoT, deterministic switches, scheduling and wireless networks, the SDN control-plane, and cyber-security, which have been cited hundreds of times as prior art in subsequent US patents. He is currently a consultant working with industry. He is listed in the top 2% of researchers in the field of "Networking and Telecommunications", according to Stanford University

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.