information

IMPACT FACTOR 3.1

CITESCORE 5.8

Article

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

Ted H. Szymanski

Special Issue
Hardware Security and Trust

Edited by
Dr. Paolo Maistri

MDPI

https://doi.org/10.3390/info15040173

information

MDPI

Article

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

Ted H. Szymanski

Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4L8, 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 "Software-Defined-Deterministic 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)-based "Zero Trust Architectures" (ZTAs). Hardware-enforced access-control eliminates all congestion, BufferBloat, and DoS/DDoS attacks, significantly reduces buffer-sizes, and supports ultra-reliable-low-latency communications in the forwarding-plane. The forwarding-plane 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; (iii) Provide guaranteed immunity to external cyber-attacks, and exceptionally strong immunity to internal cyber-attacks; (iv) Save USD 100s of billions annually by exploiting FPGAs; and (v) Enable hybrid Classical-Quantum networks, by integrating a "quantum key distribution" (QKD) network with a classical forwarding plane with exceptionally strong cyber-security, determined by the computational hardness of cracking Symmetric Key Cryptography. 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

Citation: Szymanski, T.H. A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced Cyber-Security for Critical Infrastructures. *Information* **2024**, *15*, 173. https://doi.org/10.3390/info15040173

Academic Editor: Krzysztof Szczypiorski

Received: 6 February 2024
Revised: 1 March 2024
Accepted: 5 March 2024
Published: 22 March 2024

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 21st century. The future CPSs include Smart Cities, Smart Transportation and Smart Healthcare Systems, the Smart Power Grid, and Smart Manufacturing. These future CPSs will require complex electronic control systems that rely upon ultra-reliable-low-latency communications (URLLCs) for M2M traffic flows, with full immunity to cyber-attackers. URLLCs for 5G/6G wireless systems are described in [1–3]. 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 URLLC 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-IP (Internet

Protocol)", 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 four 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]. As a result of the best-effort service model, the Consumer IoT provides no guarantees that traffic will be delivered by a given deadline, or delivered at all.

Figure 1a illustrates a Venn-like diagram, with the Consumer IoT, the Industrial IoT, Cyber-Physical Systems, and Industry 4.0. The next-generation IoT will comprise two 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 [10]). Kleinrock proposed a "Narrow-Waist" model for the protocol stack of the Consumer IoT three decades ago in 1994, which has not significantly changed in three decades. IP suffers from several serious cyber-security vulnerabilities that have existed in layer-3 for several decades. It uses: (i) unencrypted IP packet headers; (ii) unauthenticated IP packet headers; (iii) middle boxes to perform address translation; (iv) Domain Name Servers (DNSs) to perform address resolution; and (v) insecure layer-3 routing protocols. 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).

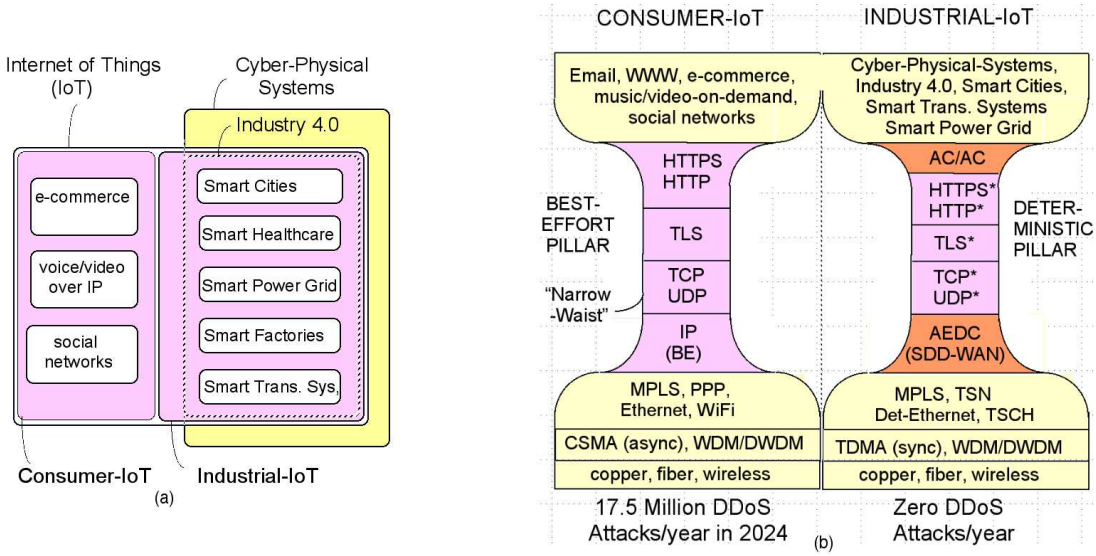


Figure 1. (**a**) Venn -like diagram illustrating the next-generation IoT, comprising the Consumer IoT and Industrial IoT, Cyber-Physical-Systems, and Industry 4.0. (**b**) A proposed "Dual Pillar" model of the next-generation IoT with a "Wider-Waist", which supports a best-effort (BE) pillar (using IP), and a deterministic pillar (using FPGAs and no IP). The deterministic pillar includes an AI-based "Admission-Control/Access-Control" (AC/AC) system to control access to network bandwidth. The deterministic pillar establishes "Authenticated Encrypted Deterministic Channels" (AEDCs) in hardware to replace IP in layer-3.

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 [11,12]. 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 to flood 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 (Hypertext Transfer Protocol) 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 h 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 January 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 USD 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 (Transmission Control Protocol) Middlebox Reflection" DDoS attacks, 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 ≈USD 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 deep cyber-security crisis, which grows deeper every year.

In 2008, the US "National Academy of Engineering" (NAE) identified 14 "Grand-Challenge" problems for the 21st century. The solutions to these problems include achieving the following: (i) clean water for the world; (ii) carbon sequestration; (iii) fusion energy; and (iv) "Security in Cyberspace" [13]. "Security in Cyberspace" has been the subject of considerable research worldwide for many years [14–23]. Many innovative approaches are being explored, i.e., Artificial Intelligence (AI), Machine Learning, Deep Learning, and Blockchain; however, the cyber-security crisis persists. The world is also exploring quantum technologies to address the cyber-security crisis, including the following: (i) quantum key distribution (QKD) networks, and (ii) hybrid Classical-Quantum networks. In principle, QKD networks can deliver "perfectly secret" keys to users guaranteed by the laws of physics, and achieve ultimate security. However, QKD networks have several vulnerabilities (i.e., to DoS and internal cyber-attacks), and the US National Security Agency (NSA) does not recommend their use (see Section 5) [24,25]. The US DARPA (Defense Advanced Research Projects Agency) initiated a research program in 2023 to explore whether a hybrid Classical-Quantum network that blends classical and quantum communications can "produce a scalable, vastly more secure networking infrastructure".

This paper explores hardware-enforced cyber-security to address the NAE grand-challenge problem of "Security in Cyberspace" for critical infrastructure. It explores a layer-3 "Software-Defined-Deterministic Wide-Area Network" (SDD-WAN) architecture which avoids the use of IP and all its vulnerabilities. It can provide hardware-enforced guaranteed immunity to external cyber-attacks, and exceptionally strong immunity to internal cyber-attacks, for critical infrastructures. (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). It is shown that the SDD-WANs can offer comparable security to QKD networks in practice, secured by the computational hardness of cracking Symmetric Key Cryptography (SKC). Hence, the SDD-WANs can provide a solution to today's cyber-security crisis, until that future time when QKD networks are ready to be deployed on a large-scale to millions/billions of users worldwide in a cost-effective manner (see Section 5).

The solutions proposed in this paper allow nations to significantly strengthen their national security by interconnecting critical infrastructure exclusively using the Industrial IoT shown in Figure 1, and completely bypassing the Consumer IoT and IP. 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. For example, every government department with sensitive

information (i.e., the Department of Defense or Department of National Security) could configure its own D-VPN, to achieve security comparable to that of QKD networks in practice. These D-VPNs are completely isolated from each other, and from the Consumer IoT.

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 [26]. 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 [27]. 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 four key attributes:

(1) Ultra-high reliability/availability, with at least 99.999% availability (with less than 1 h 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 four goals. The next-generation IIoT, if it can meet these four 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 USD 100 trillion in economic activity.

Figure 2 illustrates a critical infrastructure of the European Union, the "Trans-European Transport Network", comprising the main transportation corridors which include roads and railways. These corridors will support future "Smart Transportation Systems", with 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 cyber-crime were ≈USD 1 trillion in 2020. The firms Cybersecurity Ventures and Statistica estimate that the global costs of cyber-crime will be ≈USD 10.5 trillion and USD 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. The "Trans-European Transport Network", a critical infrastructure spanning the EU. The bold lines of different colors represent different "Corridors"; Yellow lines indicate the Altantic corridor. Green lines indicate the Mediterranean corridor. Please see European Commission, Department of Mobility and Transport, Transport Themes (https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment_en, accessed on 1 March 2024).

Table 1. Some Critical Infrastructures in the USA.

Sector	Features
Chemical	Hundreds of thousands 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 and cyber-attacks. Comprises metals, machinery, electrical, and 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, and natural gas resources, to ensure energy for the nation. CRITICAL (enables all other sectors). Over 6400 power plants generating over 1 Terawatt of power. Numerous pipelines to distribute fuels.
Nuclear reactor	Ninety-two active reactors generate 20% of US energy. Eight fuel facilities, producing Uranium-235 for reactors. Over 3 million shipments/year of radioactive materials.
Water and 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.

The Forwarding-Plane: As shown in Figure 1b, the deterministic pillar introduces a new forwarding-plane (i.e., sub-layer-3a) to support M2M communications. The forwarding-plane can implement "Authenticated and Encrypted Deterministic Channels" (AEDCs), which are also called "deterministic traffic flows " (D-flows), directly in hardware. The forwarding-plane comprises a "Software-Defined Networking" (SDN) control plane and many 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 AEDCs, through a network of 1000 s of authenticated D-switches realized with FPGAs, to enable the ultra-reliable-low-latency communications needed for critical infrastructure.

Two unique aspects of the proposed SDD-IIoT 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)-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. All other communications do not have reservations and are anomalies, i.e., malicious packets due to cyber-attackers; (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 100 s 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 [28–31]. Reference [29] explored the hardware implementations of cryptographic functions, and identified two very important techniques to combat IoT vulnerabilities: (i) redundancy of hardware; and (ii) redundancy of information.

This paper exploits these two 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) Access Control eliminates all congestion, BufferBloat, and DoS/DDoS attacks [32–36];
(2) It reduces buffer sizes in D-switches by factors of 100,000+ times, relative to a BE-IP router [32–36];
(3) It reduces end-to-end layer-3 delays to "Ultra-Low Latencies" (ULLs), i.e., the speed-of-light in fiber; [32–36];

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 [32];
(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 [32].
(6) The global costs of cyber-crime to society, estimated to exceed USD 10 trillion annually (in 2025), can be significantly reduced [32].
(7) The global cost savings in layer-3, achieved by introducing SDN, FPGAs, and determinism into layer-3, can reach USD 100s billions per year (see Section 7). This result improves upon the estimated savings of USD 10s of billions per year presented in [32].
(8) The security of an SDD-WAN is significantly improved compared with existing classical networks, and is determined by the computational hardness of cracking Symmetric (secret) Key Cryptography (SKC) (see Section 5).
(9) The SDD-WANs can enable a hybrid Classical-Quantum network by integrating a QKD network with a classical forwarding-plane with "authenticated channels" with full-immunity to external cyber-attacks (see Section 5). It is well-known that QKD networks require "authenticated classical channels" for control [37].
(10) According to the US "National Security Agency" (NSA), QKD networks suffer from several vulnerabilities. The solutions typically require the use of Symmetric Key Cryptography, which lowers the security of QKD networks to the computational hardness of cracking SKC. As a result of these vulnerabilities, 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 future time when QKD networks are ready to be deployed on a large-scale to millions/billions of users worldwide at a reasonable cost (see Section 5).

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 [32]. These benefits are repeated here for completeness. Related papers on a deterministic IoT were presented in [33–36]. Reference [32] 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 "Wider-Waist", comprising a best-effort pillar for the Consumer IoT, and a deterministic pillar for the Industrial IoT. It presents an updated flowchart for the SDN control plane, which includes the following: (i) the IETF (Internet Engineering Task Force) "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 a forwarding-plane using Intel STRATIX FPGAs. It establishes that the FPGA hardware can detect cyber-attacks within 10–100 s of billions of Gigabytes of Internet traffic per day, which is well above the capacity of the global Consumer IoT in 2024. It shows that, in practical deployments, the SDD-WANs have comparable cyber-security to QKD networks (see Section 5). It presents extensive experimental results for an 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. Appendix A includes a list of common abbreviations used in the paper, and 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

Table 2 illustrates several vulnerabilities of layer-3 IP that have existed in the Consumer IoT for many decades. The Consumer IoT provides a "best-effort" (BE) service to billions of IoT devices/computers [6]. According to Cisco, there will be about 33 billion IoT devices generating about 10 billion Gigabytes of traffic/day in 2024 [11,12]. Unfortunately, the Consumer IoT does not provide any "Admission-Control/Access-Control" (AC/AC) 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") performs routing in the Consumer IoT. However, BGP routing 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, the 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.

Table 2. Vulnerabilities of layer-3 IP in the 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. A 4 Tbps IP router with a 1/4 s delay requires 1 Terabit buffer. Impossible to fit a BE-IP router with 4 Tbps capacity onto a single FPGA.
Un-encrypted and Unauthenticated IP packet headers	IP uses unencrypted and unauthenticated packet headers. IP 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.

Table 2. *Cont.*

Vulnerability	Summary
Layer-3 routing	Layer-3 routing is performed in every BE-IP router. A router processes unencrypted and unauthenticated IP packet headers. Routing is insecure. Cyber-attackers can easily re-route traffic to a destination they control.
Middle boxes	Middle boxes perform essential functions, i.e., address translation, Intrusion Detection Systems, and firewalls. Middle boxes are also insecure.
Domain Name Servers (DNSs)	Domain Name Servers perform essential functions, i.e., address-resolution. DNSs are also insecure.
DoS and DDoS attacks	A cyber-attacker in a compromised middle boxes 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 are among "the most significant weapons on the Internet". ≈17.5 million DDoS attacks occurred in the Consumer IoT in 2024 (Cisco). The average DDoS attack lasted for 8 h in 2022 (Cloudflare).
"Isolation control"	Cannot isolate sub-networks within the BE-IP, to contain cyber-attacks.
Over-provisioning	The IoT is "over-provisioned" and operates at ≤40% of peak capacity; ≥60% of IoT capacity is unused (for very-high capital and energy costs).

2.1.1. The Narrow-Waist Best-Effort Service Model

Six protocols form the "Narrow-Waist" of the Consumer IoT, as all traffic must pass through these protocols [38–41]. As shown in Figure 1b, these six protocols include the following: (i) IP (Internet Protocol); (ii) TCP (Transmission Control Protocol); (iii) UDP (User Datagram Protocol); (iv) TLS (Transport Layer Protocol); (v) HTTP (Hypertext Transfer Protocol); and (vi) HTTPS (HTTP-over-TLS). As a result of the "Narrow-Waist" model, all Consumer IoT traffic inherits the weaknesses of IP, i.e., the reliance on a best-effort service model, the lack of deterministic QoS guarantees, and the vulnerability to layer-3 cyber-attacks, especially DoS/DDoS attacks.

The layer-4 TCP will guarantee that any data are delivered in the correct order. The TLS protocol will provide "cryptographic security" for end-to-end traffic flows [42]. ("Cryptographic security" can be defined as immunity to cryptographic attacks which attempt to perform eavesdropping, message tampering, and message forgery [42]). 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.

2.1.2. DDoS Attacks against Servers and Networks

DoS/DDoS attacks warrant special attention, as they are considered by the 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, Consumer IoT traffic can be delayed by seconds, minutes, hours, days, or weeks, or may never be delivered at all. DDoS attacks are discussed in [43–51].

There are two 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.

2.1.3. TLS—Does It Provide Security or Confidentiality?

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.

Table 3. Does "Transport Layer Security" (TLS) provide security or confidentiality?

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 [42]	"TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery".
IEEE [52]	"TLS is possibly the most used protocol for secure communications, with a 18-year history of flaws and fixes".
ACM [53]	TLS "is the defacto standard for secure communication on the internet".
Source	Quotes questioning TLS security.
NIST [54]	"There are no known ways to prevent flooding DoS attacks against hosts visible on the Internet".
IEEE [48]	"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".
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	Confidentiality: "The state of keeping or being kept secret or private".

According to the Internet Society, TLS provides "end-to-end security" for data sent over the Internet. According to the US NIST (National Institute for Standards in Technology), TLS provides a "safe communications channel" over the Internet. According to the IETF, TLS prevents "eavesdropping, forgery and message tampering" [42]. According to a 2020 ACM (Association for Computing Machinery) paper, "TLS is the defacto standard for secure communication on the Internet".

The security of TLS is established in several theoretical papers, i.e., [52,53,55,56]. These papers establish that TLS is "secure", given very specific assumptions about the types of cyber-attacks that could occur on 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 [55] defines the "security" of TLS as follows: (i) The protocol includes a secure authentication phase; and (ii) all data are transmitted using "Symmetric Key Cryptography" (SKC), to ensure their confidentiality. Hence, these proofs of "security" imply that the data are securely transmitted, and that 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.

It is very important to note that TLS "cryptographic security" established in [52,53,55,56] does not imply immunity to DoS/DDoS attacks. DDoS attacks have been around since 1996, and the importance of DDoS attacks was highlighted in a 2004 paper [43]. 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" [54]. According to the firm Norton, DoS/DDoS attacks are one of the most "significant weapons on the Internet". According to Cisco, there will be ≈17.5 million DoS/DDoS attacks on the Consumer IoT in 2024. Hence, the reader should note that the "TLS Security" established [52,53,55,56] implies "cryptographic security", rather than general immunity 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) did not exist, and their proofs of "security" do not apply to the Consumer IoT.

Unfortunately, the TLS protocol suffers from several vulnerabilities [57–61]. 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 even 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" against arbitrary external cyber-attacks, as the TLS traffic might be delivered very late, or never at all. This paper argues that TLS provides excellent "confidentiality", but limited "security" to all types of cyber-attacks. Having accurate definitions is important, given the significant costs that society incurs due to cyber-attacks.

2.1.4. TLS—Provides 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 (typically called a "Remote Code Execution" attack). In the "LOG4J" attack, a cyber-attacker can take control of secured web-server by exploiting a vulnerability in the Apache Software Foundation software that such web-servers typically use (as first reported in 2021). The use of TLS (i.e., HTTP-over-TLS) 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 detect the cyber-attack. (Please see [32] for more details on this cyber-attack, and how it is mitigated).

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 4 were using HTTPS by 2014, given Yahoo's experience. However, it is clear that even with the widespread use of HTTPS and TLS (as in HTTP-over-TLS), large external cyber-attacks still occur frequently, where the data of 100 s of millions of users are compromised.

Table 4. World's 10 largest reported data breaches (CSO online, 30 November 2022). (See https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, accessed on 10 March 2024).

Service	Date	Description	External/Internal
Yahoo	August 2013	3 billion accounts	External
MySpace	2013	360 million accounts	External
Yahoo	2014	500 million accounts	External
Adult Friend Finder	October 2016	412 million accounts	External
Aadhaar	January 2018	1.1 billion accounts	External
Marriott International	September 2018	500 million accounts	External
Facebook	April 2019	533 million accounts	Internal
Alibaba	November 2019	1.1 billion pieces of user data	Internal
Sina Weibo	March 2020	538 million accounts	External
LinkedIn	June 2021	700 million accounts	External

In summary, according to Internet Society, TLS provides "end-to-end security" for data sent between applications over the Internet, but this statement is imprecise. The "security" TLS achieves is "cryptographic security", which 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 "confidentiality" but provides relatively weak "security" against general cyber-attacks, especially DoS/DDoS flooding attacks, which are considered among the most "powerful weapons on the Internet".

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 as follows: 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 Consumer 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 five 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 five deterministic protocols. Any application programs in the Industrial IoT wishing to use these deterministic protocols must first receive prior 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, and 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 and Intrusion Detection Systems

A significant amount of research over the last decade has addressed the cyber-security crisis [14–23]. "Access-Control" systems limit the access to critical resources, typically using AI rule-based policy engines [62–65]. In 2021, the US government issued 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 substantial adaptation of ZTA principles is required by the end of 2024. 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. Access-control systems can significantly reduce the vulnerability to external and internal cyber-attackers, by adding rules to control access.

"Intrusion Detection Systems" (IDs) are also critical to secure the Consumer IoT. These systems typically reside in a hardware "middle box". They process traffic flows, examining the byte-sequences using "Deep Packet Inspection" (DPI), looking for the "signatures" of a known cyber-attacker. The introduction of IDS middle boxes significantly increases the capital costs of the Consumer IoT, as well as 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].

2.4. Cryptography

2.4.1. Symmetric (Secret) Key Cryptography (SKC)

In SKC, the sender and receiver shared 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 [83].

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 [84,85]. However, even with a super-conducting Quantum Computer, Grover's algorithm requires billions of years to crack AES-256 [32]. Hence, the NIST AES-256 security level is considered quantum-safe. The Chacha20 Stream cipher is also considered quantum-safe.

2.4.2. "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 [86]. For proven security, encryption uses the Chacha20 cipher, and authentication uses a Poly1305 message authentication code [83]. AEAD is used in Google Chrome and FireFox web-browsers, and in TLS version 1.3. The SDD-WANs can also use AE/AEAD.

2.4.3. "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 [24,87].

2.4.4. Post-Quantum Cryptography (PQC)

In 2016, the US NIST started a project on PQC [88]. 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 three rounds of competition, in July 2022. Status reports on each round are available from the NIST and ETSI websites. The results of round 3 are presented at [89]. In the class of public key encryption algorithms, the CRYSTALS–Kyber submission was selected. In the class of digital signature algorithms, three 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 [90]. 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.

2.5. QoS Guarantees in the IoT

2.5.1. QoS Guarantees for Best-Effort Traffic

The problem of achieving QoS guarantees (on the delivery, latency, and throughput) for competing best-effort traffic flows in the Consumer IoT is well studied [91–95]. Two switch architectures for BE-IP routers are popular, namely (i) the "Input-Queueing" (IQ) and (ii) the "Combined Input and Output Queueing" (CIOQ) architectures. The design of packet buffers for BE-IP routers is explored in [96,97]. Scheduling algorithms are explored in [98,99]. Unfortunately, links in the Consumer IoT typically experience excessive delays of 100s of milliseconds. To mitigate delays, layer-3 links typically operate at light loads between 20 and 30% [100,101].

2.5.2. IEEE and IETF Activities for Improved QoS

The IETF had explored ways to achieve a high "Quality of Service" (QoS) in the Consumer IoT in the 1990s with the "Integrated Services" and "Differentiated Services" service models [102,103]. However, these IETF models were based on a "best-effort" communications paradigm, and did not provide deterministic services.

The IEEE 802.1 Working Group presented a tutorial on a "Deterministic Ethernet" (D-Ethernet) network in 2012 [104]. The IEEE proposed a "Time-Slotted Channel Hopping" (TSCH) technology for wireless networks in 2012 [105]. 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 proposed a deterministic wireless network based upon TSCH in [106].

The IETF DetNet group also proposed a "converged WAN" that in principle could support both best-effort and deterministic traffic flows [107–109]. The DetNet converged WAN retains many vulnerabilities that have existed in layer-3 IP networks for many decades. It uses: (i) unencrypted and (ii) unauthenticated IP packet headers (iii) middle boxes, (iv) insecure layer-3 routing; and (v) insecure layer-3 Domain-Name-Servers. Huawei has also reported a deterministic IP network in [110]. It also retains many vulnerabilities that have existed in layer-3 IP networks for many decades, as stated above. These networks are thus vulnerable to layer-3 cyber-attacks, i.e., Spoofing cyber-attacks (in which an unencrypted IP packet header is modified) and DoS/DDoS cyber-attacks.

2.5.3. 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 [111]. The IEEE has developed a list of desirable features for an ultra-low-latency "Tactile Internet" [112]. The IEEE proposed "Time-Sensitive Networks" (TSN) as a step towards achieving ultra-low-latency networks [113].

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.

2.5.4. Birkhoff–von Neumann (BVN) Stochastic Matrix Decomposition

A theoretical frame-work for scheduling deterministic traffic flows through a crossbar switch is given by the "Birkhoff–von Neumann" (BVN) bistochastic matrix decomposition

algorithm [114,115]. Consider an N × N 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 N × N "Traffic Rate Matrix" T. The Birkhoff–von Neumann theorem established in 1946 states that a doubly stochastic traffic rate matrix T can be decomposed and expressed as a weighted sum of permutation matrices.

Over 50 years later and in a significant advancement of theory, a deterministic crossbar switch using the BVN algorithm to schedule traffic was first proposed in 2001 [114]. However, its performance was sub-optimal. It had a very large computational complexity (runtime) of $O(N^{4.5})$ time, the length of the scheduling-frame F was very large ($O(N^2)$ time-slots), and the maximum "service-lag" was very large ($O(N^2)$ 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 attempted to 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 [116]. 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" [117]. Researchers at UC Riverside established a jitter bound that grows with the switch degree $O(N)$, and stated an open problem on the BVN scheduling of deterministic traffic: "to determine the minimum speedup required to provide hard guarantees, and whether such guarantees are possible at all" [118].

2.5.5. 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 [119–121]. 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 [122–124].

The Deterministic IIoT uses an innovative algorithm to decompose a Birkoff–von Neumann (BVN) bistochastic traffic rate matrix T, called the "Recursive Fair Stochastic Matrix Decomposition" (RFSMD) algorithm [33,119]. 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 bistochastic traffic rate matrix to yield a provable optimal-order deterministic delay and jitter guarantees [33,119]. This RFSMD algorithm results in the ultra-low latency of the D-IIoT (please see Section 6).

A "Deterministic IIoT" was also explored in [34], 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 USD 10s of billions/year. Additional results were reported in [33,35,36].

A Deterministic IIoT, in which the routing and scheduling functions are migrated into the SDN control plane, was proposed in [125]. This migration eliminates several cyber-security vulnerabilities that have existed in layer-3 (IP) of the Consumer IoT for many decades: the use of (i) unencrypted IP packet headers; (ii) unauthenticated IP packet headers; (iii) middle boxes; (iv) insecure layer-3 routing, and (v) Domain Name Servers.

The elimination of these cyber-security vulnerabilities thus improves cyber-security in the IoT, as proposed in [126].

2.6. 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 ms will require a worst-case buffer size of ≈1 terabit of memory. Assuming an average IP packet size of 1000 bytes, the transmission link requires a worst-case buffer size of ≈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.

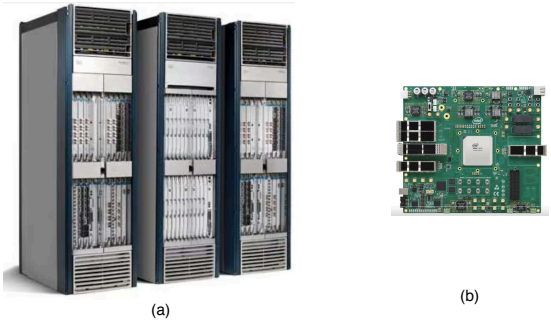
However, it has been shown that the use of determinism can eliminate "BufferBloat" and reduce buffer sizes by a factor of ≈100,000+ times [32,36]. The same transmission link, using determinism, may require a worst-case buffer for ≈1250 packets. Hence, a simple authenticated D-switch can be created using 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 routers 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 [32–34,36];
(3) D-switches do not need gigabytes of high-speed memory 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.

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 ≈USD 7500 USD per FPGA. A D-switch with ≈3.5 Tbps capacity can fit on one FPGA, and consume ≤ 225 watts. Please see Figure 3 on the impact of FPGAs.



(a) (b)

Figure 3. (**a**) Three chassis of a Cisco Carrier-Routing-System 3 (CRS-3), available in 2014, each with a capacity of ≈4.5 Terabits per second (Tbps). One CRS-3 chassis occupied 56 cubic feet of volume, weighed

1630 pounds, and consumed 7.66 kW of power. (See www.cisco.com, accessed on 8 March 2024). (**b**) A Printed Circuit Board (PCB) with one Intel STRATIX-10 Field Programmable Gate Array (FPGA) integrated circuit, with a capacity of ≈3.5 Tbps, available in 2024. The PCB occupies less than 1 cubic foot of volume, weighs less than 2 pounds, and consumes ≈225 watts. FPGAs represent an unprecedented opportunity for innovation, if they can be utilized effectively in layer-3. (See www.digikey.ca, accessed on 8 March 2024).

3. The Deterministic IIoT—Key Features

Figure 4a illustrates layer-3 which supports best-effort traffic in the Consumer IoT, which comprises many BE-IP routers and middle boxes. Figure 4a also illustrates sub-layer-3a which supports M2M traffic in the Industrial IoT, which comprises an SDN control plane and a forwarding-plane with many D-switches, realized with FPGAs. The SDN control plane performs the tasks of routing and scheduling traffic in the sub-layer-3a, and hence the D-switches are much less complex compared to layer-3 BE-IP routers.

Figure 4b illustrates an SDD-WAN spanning the European Union, with 28 nodes (cities) and 82 edges. In Figure 4b, the SDD-WAN can be represented by a graph G(V,E) with vertices V and edges E. Each city has one vertex (i.e., a D-switch), with fiber-optic edges to its nearest neighbours (other D-switches). In Figure 4b, the solid black lines represent the fiber-optic edges between cities in layer-3, and the dotted lines represent ultra-low-latency D-flows between the cities in the sub-layer-3a. 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 the layer-3 efficiency and security.

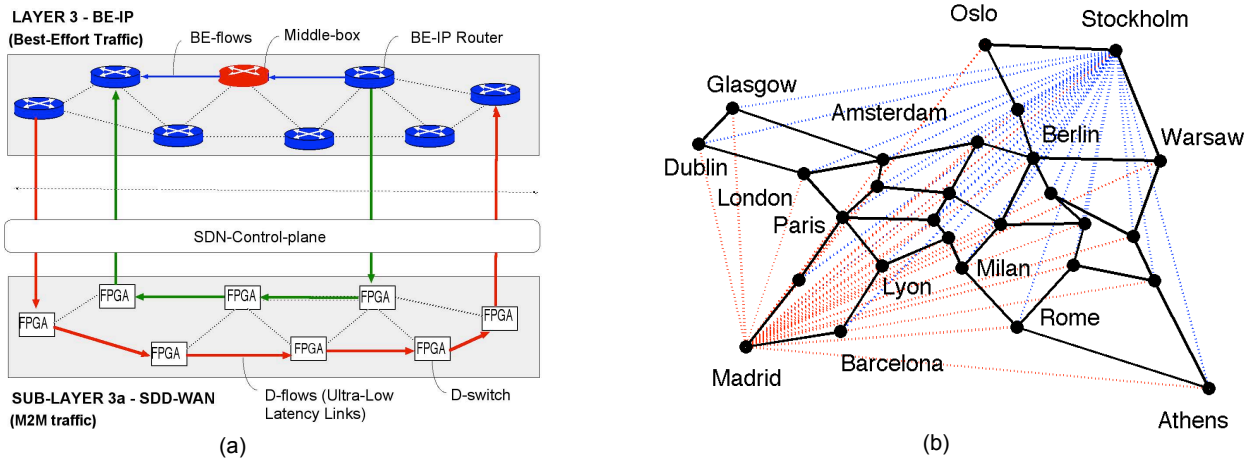


Figure 4. (**a**) The Consumer IoT resides in layer-3 and comprises several BE-IP routers and middle boxes. The Industrial IoT resides in sub-layer-3a, and comprises an SDN control plane and a forwarding-plane of D-switches (FPGAs). (**b**) An SDD-WAN spanning the European Union with 2 D-VPNs. Madrid has a D-VPN with a D-flow to every node in the EU, as shown in red. Stockholm has a D-VPN with a D-flow to every node in the EU, as shown in blue. Solid black lines denote fiber-optic edges in layer-3. Dotted lines denote ultra-low-latency D-flows in sub-layer-3a, which bypass layer-3.

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. A "Deterministic Traffic Source" (D-source) will inject a deterministic traffic flow into the SDD-WAN, under the control of the SDN control plane. A "Deterministic Traffic Sink" (D-sink) will receive a deterministic traffic flow from the SDD-WAN, under the control of the SDN control plane. A "Deterministic Transceiver" (D-transceiver) comprises a D-source and a D-sink. A "Deterministic Packet Switch" (D-switch) receives deterministic traffic

flows on incoming fiber-optic edges, and forwards these traffic flows to outgoing fiber-optic edges, under the control of 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): (i) the IIoT Controller; (ii) the WAN Controllers; and (iii) the 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 Deterministic Channel"). All 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 unauthorized 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 two 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 the 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 rate (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 downloads 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 rate 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 downloads 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 a sub-layer 3a, and the D-sinks can re-assemble the larger packets (each cell must pass an "authorization check", explained subsequently, and will thus need a sequence number and a CRC checksum for error detection).

3.5. Deterministic VPNs (D-VPNs)

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 (or enterprise servers) 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) be completely encrypted. An encrypted DVN is called a "Deterministic Virtual Private Network" (i.e., a D-VPN).

In Figure 4b, two 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 network. These D-VPNs are completely isolated from each other, and from the Consumer IoT.

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 entitled "Improving the Nation's Cybersecurity" [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., to 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 include 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 the following: 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 for 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 databases 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 [32] 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 ≈ 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 [86]. In addition, each D-source can maintain a counter with ≈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 1000s 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.

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 5. 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 the input port (j) and depart from the output port (k). Each output port k has N "Output Queues" (OQs), where OQ(j,k) buffers one or more packets which arrive at input port (j) and will depart from output port (k). (The LFSRs (Linear Feedback Shift Registers) are optional—they can be used to "randomize" the traffic on each link).

The NxN D-switch in Figure 5 has five controllers: (i) IP-CNTRL-1 directs incoming packets arriving 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 an 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 VOQs supported by the switch.

In Figure 5, all of the controllers can use control-vectors 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 control-vectors 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 [32]: (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 routing protocols, i.e., BGP, which add significant costs and security vulnerabilities to a BE-IP router.

In Figure 5, the output queues are typically used to re-assemble larger IP packets from many smaller "cells" of data sent through the crossbar switch. In the SDD-WANs, IP packets are not used and hence the output queues are not necessary. The switch in Figure 5 can be simplified, as any "cell" of data arriving at an output port can be immediately transmitted onto the outgoing fiber, thereby eliminating the need for output queues and two controllers at each output port.

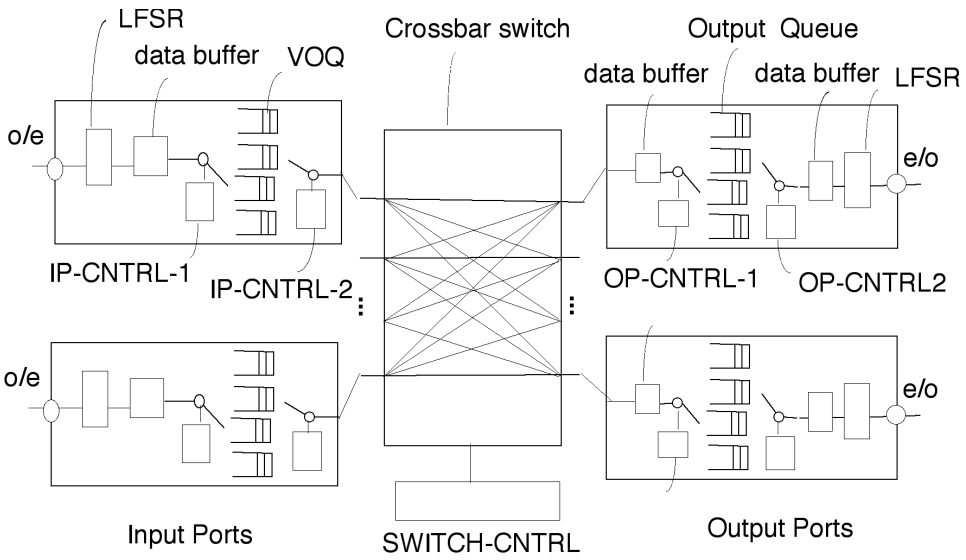


Figure 5. A Combined Input and Output Queued (CIOQ) D-switch with 5 deterministic controllers. An N × N switch has N input ports and N output ports, interconnected with an unbuffered N × N crossbar switch. Each input port has N Virtual Output Queues (VOQs), and each output port has N output queues. The controllers store pre-computed control-vectors, to control the operation of the D-switch.

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 whether one (or more) rules exist to approve the D-flow. If the request is approved, then the SDN control plane will perform several tasks for the new D-flow. It will pre-compute the following: (i) the end-to-end routing; (ii) the end-to-end scheduling; (iii) the D-schedules for all traversed edges; and (iv) the quantum-safe keys for AE of the D-flow. The SDN control plane will then download the 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 [32]. 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 an SOF signal/packet from each neighbour roughly once every millisecond (depending upon the duration of a scheduling-frame).

3.8. Using MPLS-like Flow Labels in Sub-Layer 3a

"Multi-Protocol Label Switching" (MPLS) WANs are often used in the Consumer IoT. An MPLS-WAN consists of an MPLS control plane, and a forwarding plane of many MPLS

packet switches, similar to Figure 4a. 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 incoming flow label, the outgoing flow label, and the desired output port. The D-switches can be modified to perform some simple packet header processing in the forwarding plane (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 incoming flow label. When a packet arrives at an input port, its flow label is extracted, and 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 flow tables can also allow for flow aggregation and flow segregation. Two incoming D-flows with deterministic date rates of R_1 and R_2 can be aggregated into one outgoing D-flow, with a deterministic data rate equal to $(R_1 + R_2)$. Similarly, one incoming D-flow with a deterministic data rate of $(R_1 + R_2)$ can be segregated into two outgoing D-flows, with deterministic data rates equal to R_1 and R_2. 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 includes 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.

3.9. D-Switches and D-Transceivers Secured with Quantum-Safe Ciphers

This section explores the security of the D-switches/D-transceivers, which are the key hardware components of the SDD-WAN. The attack surface must be carefully minimized, to ensure the security of the SDD-WAN.

The D-switches/D-transceivers are Finite-State Machines, where the behaviour is exclusively determined by the control vectors stored in the five controllers, as shown in Figure 5. To minimize the attack surface, the D-switches/D-transceivers: (1) do not use a Linux-based operating-system that can be compromised; (2) do not execute software (i.e., Java code) stored in memory that can be compromised; (3) do not run insecure layer-3 protocols (i.e., layer-3 routing protocols such as BGP) that can be compromised; (4) do not run insecure layer-3 Berkeley–Sockets user-programmable software that can be compromised; (5) have their functionality "burned into" the FPGA hardware, i.e., their functionality is immutable.

A D-switch/D-transceiver has several optical Input/Output (IO) ports, and one electrical IO port. A D-switch receives optical packets on each optical input port, as specified in a D-schedule associated with each input port. A D-schedule identifies the time-slots in which authorized optical packets may arrive at each input port. Any optical packets arriving at any other times are unauthorized and are labelled as anomalies, i.e., malicious packets. All arriving packets must pass the authorization check, i.e., each packet is decrypted using a quantum-safe cipher (i.e., using the IETF Authenticated Encryption (AE) algorithm).

The D-switch is configured with control packets sent from the SDN control plane. These control packets must pass the authorization check, i.e., they will be decrypted using a quantum-safe AE key. If a control packet passes the authorization check, it can update the state of the D-switch.

There are several types of allowable control packets to update the state of a D-switch:

(1) Reset all the controllers to a known initial state.
(2) Update the control vector for one specific controller.
(3) Reset the flow table to a known initial state (if a flow table is used).

(4) Write a new row of data into the flow table (if a flow table is used).
(5) Update a D-schedule for an input port.

The D-switch contains one electrical IO port, which is used for initialization when the switch is "powered up". It can receive electrical control-packets from an external secured controller to achieve a known initial state. The electrical control packets must also pass an authorization check. The D-switch can be assigned a pre-shared secret key (PSK) to be used in the authorization check of control-packets on the electrical IO port. Alternatively, every D-switch can be pre-assigned a unique private key for decrypting control packets. A secured controller can use a public key to encrypt a control packet sent to each D-switch.

The analysis of the security of a system typically allows for several assumptions. (1) A large system comprises two types of components, "secured" components and all other "unsecured" components. (2) The "secured components" are truly secure, and free of internal cyber-attackers. The administrators of secured systems must employ the most-advanced technologies to detect and remove internal cyber-attacks within secured components, i.e., they must employ intrusion detection systems (IDSs) to detect intruders, and they must employ Zero Trust Architectures (ZTAs) to control access to critical resources.

To eliminate virtually all internal cyber-attackers, rules can require the approval of multiple persons to perform a critical task, and rules can require biometric data of each person. Approval may be needed from the employee, their immediate supervisor, the director of the division, and the president of the company. Such rules would eliminate the possibility of a single intruder/internal cyber-attacker (i.e., with access to one employee's passwords) having access to any critical components. We use these assumptions to establish the following property.

Property 1. The security of D-switches: The probability that a malicious packet generated by an external cyber-attacker can compromise a D-switch is effectively zero, i.e., the expected number of times a malicious packet from an external cyber-attacker can compromise a D-switch per year is zero.

Proof: The attack surface has been minimized. A D-switch does not use operating systems, software (i.e., Java code), or insecure layer-3 routing protocols, i.e., the Border Gateway Protocol (BGP), which can be compromised. A D-switch is a Finite-State Machine with only two possible types of Input/Output (IO) ports, namely optical and electrical IO ports. The behaviour of the D-switch is only controllable by control packets received on an IO port. The D-switch only accepts control packets that pass an authorization check, and this behaviour is embedded in hardware and is immutable. All other data and packets are discarded. To pass an authorization check, a control packet must be successfully decrypted using a quantum-safe cipher, and the message integrity must be ensured, i.e., the message authentication code (MAC) must be verified.

A super-conducting Quantum Computer can use Grover's quantum search algorithm to crack a quantum-safe cipher [84,85]. Using a K-bit secret key, the number of quantum queries required in Grover's search is $\sqrt{2^K}$. In a super-conducting Quantum Computer, the minimum time to perform any quantum operation (i.e., a quantum logical operation) is ≈10 nanoseconds. A quantum query of the AES algorithm will take much more time. Using a quantum-safe key with 256 bits, the expected number of Quantum queries using Grover's algorithm is $\sqrt{2^{256}} = 2^{128} \approx 10^{38.5}$ queries. Given that each query requires at least 10 nanoseconds, the minimum time to crack the cipher is $\approx 10^{30}$ seconds. The current life of the universe is estimated at 13.787 billion years, equivalently about 10^{20} seconds. Hence, there is not enough time in the life of the universe, for a super-conducting Quantum Computer to crack a quantum-safe cipher with 256 bit keys, using Grover's quantum search algorithm. The expected time needed to crack a quantum-safe cipher with 256 bits using a superconducting Quantum Computer is billions of times the life of the universe. The probability that an external cyber-attacker can compromise a D-switch is effectively zero. Q.E.D.

A similar property holds for D-transceivers, and is stated without proof next.

Property 2. The security of D-transceivers: The probability that a malicious packet generated by an external cyber-attacker can compromise a D-transceiver is effectively zero, i.e., the expected number of times that a malicious packet from an external cyber-attacker can compromise a D-transceiver per year is zero.

4. The SDN Control Plane

Figure 6 illustrates a flowchart for the SDN control plane, for an SDD-WAN using IQ or CIOQ switches (the control plane for crosspoint-buffered switches is similar). This flowchart upgrades an earlier flowchart first presented in [32], 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, thus eliminating many cyber-security vulnerabilities that have existed in layer-3 of the Consumer-IoT for many decades. D-switches do not examine unencrypted and unauthenticated 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 vastly 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.

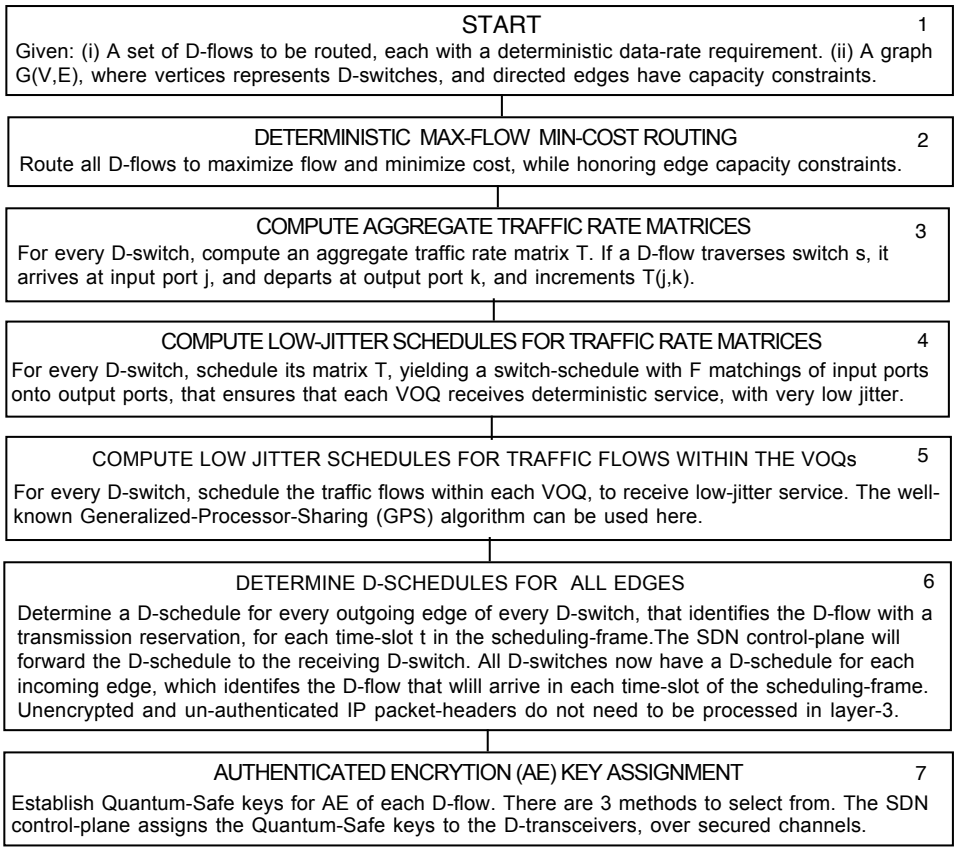


Figure 6. A concise flowchart for the SDN control plane.

The following notation will be used in Figure 6. 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 by R(f) to be satisfied. A "Maximum-Flow–Minimum-Cost" (MFMC) routing algorithm is used in the SDN control plane [122]. The algorithm optimizes aggregate throughput and minimizes costs, and can achieve up to ≈100 % utilization of edges in the 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 1000s of D-flows. This step yields a 3D array $T(j,k,s)$, where the third index identifies the D-switch s. For each D-flow f traversing the D-switch s, which arrives at the input port j and departs at output port k, the 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 to decompose a Birkhoff–von Neumann (BVN) traffic rate matrix, called the "Recursive and Fair Stochastic Matrix Decomposition" (RFSMD) algorithm [33,119]. Given an $N \times N$ doubly stochastic BVN traffic matrix $T(j,k)$, this algorithm will compute a low-jitter linear 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 a 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 the transmission that satisfies the demand 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 for scheduling the D-flows within each VOQ are given in [33]. These scheduling algorithms also minimize the jitter, which will reduce the 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 [33,124].

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 [33]. 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 receive 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, have transmission reservations on each OP k in each time slot of a periodic scheduling frame. These D-schedules will significantly strengthen the 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 the D-switch s will also become the D-schedule for the input port j of the receiving D-switch d. The SDN control plane will thus forward the D-schedule from the D-switch s (output port k) to D-switch d (input port j). A D-schedule can also identify the output port that an arriving packet requires, which will allow encrypted packets to traverse a D-switch without examining unencrypted and unauthenticated IP packet headers. Hence, D-switches do not need to examine IP packet headers, in order to make layer-3 routing decisions.

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 [127]. 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, similarly to [127,128]; (ii) The end-points can perform a post-quantum key exchange algorithm over the secured channels via the SDN control plane, similarly to [129]; (iii) The SDN control plane can generate quantum-safe keys, and assign these to the end-points over secured channels [32].

4.8. Summary—SDN Flowchart

This flowchart 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 the following:

(1) D-switches to process unencrypted and unauthenticated IP packet headers to perform insecure layer-3 routing;
(2) Many gigabytes of high-speed RAM to store insecure layer-3 routing tables for the layer-3 routing protocol BGP;
(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") and BGP;
(4) Layer-3 "middle boxes", which perform the "Network Address Translation" (NAT) needed for insecure layer-3 routing;
(5) Layer-3 "Domain-Name-Servers", which perform address resolution needed for insecure layer-3 routing.

The use of pre-computed D-schedules results in a vast simplification of the D-switches, which leads to significantly stronger security. 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.

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-WAN Properties 1 and 2, establishing the security of D-switches/D-transceivers, were presented in Section 3.

Property 3. Security of the SDN control plane: The SDN control plane is considered a "secured" component in the system, that runs in secured data centers. Administrators must use the most advanced technologies, to ensure that the SDN control plane and the data-centers remain secure (service providers such as Google, Amazon, and Apple currently use many advanced technologies to remain secure, and they are highly successful). Access to a data center supporting the SDN control plane must be controlled by a Zero Trust Architecture, as dictated by the US Presidential Order 14284 passed in 2021. The number of humans who can access the system should be severely limited, and every user must be authenticated using passwords and biometric data, when accessing any resource, however small. Access to any secured computer supporting the SDN control plane must be controlled by a Zero Trust Architecture. The administrators must run Intrusion Detection Systems to detect any possible intrusions within a data center. To eliminate the possibility of a single intruder from gaining access to any critical resources, rules could require authorization from multiple persons to enable access to a critical resource.

Property 4. Majority voting in de-centralized SDN control plane: The SDN control plane realizes an Admission-Control/Access-Control system using three 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 [130,131]. 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., three out of five copies must agree to confirm a decision (this property exploits the principles of redundancy of hardware and redundancy of information, as described in [29]). 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 5. Only authorized D-flows reserve bandwidth: A request for a new D-flow will only be approved if rules in the WAN Controller's knowledge base explicitly allow 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 "Authenticated Encryption". 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 are not forwarded.

Property 6. 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 ≈20.48 nanoseconds, and the scheduling-frame requires ≈0.672 ms.

Property 7. Routing/scheduling can achieve ≈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 [122], which can achieve ≈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 with a transmission reservation in each time slot of the scheduling frame. Using the scheduling algorithms in [33], 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 [32]. 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 8. 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 IP 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 Consumer IoT network: (a) The use of unencrypted and unauthenticated IP packet headers in layer-3 is eliminated. These headers are insecure and vulnerable to manipulation by cyber-attackers; (b) The need for insecure middle boxes to perform "Network Address Translation" (NAT) is eliminated; (c) The use of insecure layer-3 routing protocols (i.e., the Border Gateway Protocol (BGP) is eliminated; (d) The use of insecure "Domain Name Servers" (DNSs) for insecure layer-3 routing is eliminated.

Property 9. 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 that 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 that a malicious packet passes an authorization check is zero.

Property 10. The guaranteed intrusion detection system: The D-switches/D-transceivers implement a "guaranteed intrusion detection system" in FPGA hardware, where any unauthorized or malicious packet from an external cyber-attacker is detected in real time. Consider two 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 9, it will fail the authorization check and be detected. That packet is not forwarded, and the SDN control plane is immediately informed.

Property 11. Redundant paths for reliability: For mission-critical applications, each "primary" D-flow is replaced by multiple (i.e., $R \geq 3$) 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 by 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, as described in [29]). 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 12. Redundant paths for cyber-security: The redundancy technique described in property 11 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 the redundancy of hardware and the redundancy of information, as described in [29]). The probability that 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 13).

Property 13. Protecting critical infrastructure: Each nation will protect its critical infrastructures from external cyber-attacks, as shown in Table 1. Each nation will likely have multiple independent SDD-WANs, managed by independent service providers, such as Google, Apple, Microsoft, 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 exceptional cyber-security providing immunity to external cyber-attacks as a new service.

For each M2M-flow for critical infrastructure, a manager 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 that 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 the 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 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. Hence, 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 only if 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 14. 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 the 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 in 2021, which requires US industries to adopt the Zero Trust Architecture (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 the following: (i) unauthorized users; and (ii) authorized users trying to perform unauthorized tasks. Unauthorized users can be detected and eliminated by using rules that exploit biometric data. Authorized users trying to perform unauthorized 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. Vulnerabilities of QKD Networks

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 [24,25]. The "National Cyber Security Center" (NCSC) in the UK, and the "Agence nationale de la sécurité des systèmes d'information" (ANSSI) in France also do not recommend the use of QKD networks.

The US NSA outlines five vulnerabilities of QKD networks, as shown in Table 5. Several papers have also discussed these drawbacks of QKD networks [132–136].

Problem 1. QKD networks cannot authenticate the source: It is well known that QKD networks require "classical authenticated channels" for control. According to the NSA, 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 NSA, 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 14, 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) unauthorized users and (ii) authorized users trying to perform unauthorized tasks. The administration/control of the AC/AC system typically requires SKC or PQC. Hence, the security of QKD network is again limited by the computational hardness of cracking SKC/PQC.

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 NSA, 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 [133], the vulnerability of QKD networks to DoS/DDoS attacks has no clear defense.

Table 5. US NSA—5 drawbacks of QKD networks [24,25].

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 and 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 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 to large-scale quantum key distribution networks [137,138]. The ETSI (European Telecommunications Standards Institute) 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 SKC or PQC. Hence, the security of QKD network is again limited by the computational hardness of cracking SKC/PQC.

In practice, the security of QKD networks is strongly limited by the vulnerabilities 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 ultimately limited by (i) the cryptography used to authenticate the source; (ii) the cryptography used to administer the AC/AC system, necessary to control internal cyber-attackers; (iii) the cryptography used to administer the AC/AC system, necessary to control the vulnerabilities of QKD networks to DoS/DDoS flooding attacks; and (iv) the cryptography used to administer the AC/AC system, necessary to control the Key Management System. All of these weaknesses lower the security of QKD networks to the computational hardness of cracking SKC/PQC. For these reasons, the NSA in the US, the NCSC in the UK, and the ANSSI in France do not recommend the use of QKD networks.

Table 6 illustrates the vulnerabilities of several networks. The vulnerabilities of QKD networks as stated by the US NSA are labelled with a "*". The Consumer IoT, without using PQC, is vulnerable to all entries in the table. The Consumer IoT using PQC within the TLS protocol is safe from TLS cryptographic attacks, and from "Harvest-Now–Decrypt-Later" attacks. In these attacks, cyber-attackers record encrypted messages this year, and decrypt the messages a few years into the future, when sufficiently powerful Quantum Computers become available. The IETF converged WAN can interconnect smaller networks that support improved QoS, i.e., MPLS networks and TSCH networks, but it ultimately uses IP to interconnect the smaller networks. Hence, the IETF converged WAN inherits all the vulnerabilities of IP. It has the same security as the Consumer IoT using PQC, and it is vulnerable to many layer-3 cyber-attacks. In contrast, the SDD-WAN is safe to all of these vulnerabilities.

Table 6. Vulnerabilities of several networks ("Vuln". denotes "vulnerable").

Vulnerability	Consumer IoT w/o PQC	Consumer IoT with PQC	IETF Converged WAN	SDD WAN	QKD Networks	Hybrid QKD and SDD-WAN
Unencrypted IP pkt. headers	Vuln.	Vuln.	Vuln.	Safe	Safe	Safe
Unauthenticated sources	Vuln.	Vuln.	Vuln.	Safe	Vuln. *	Safe

Table 6. *Cont.*

Vulnerability	Consumer IoT w/o PQC	Consumer IoT with PQC	IETF Converged WAN	SDD WAN	QKD Networks	Hybrid QKD and SDD-WAN
Middle boxes	Vuln.	Vuln.	Vuln.	Safe	Safe	Safe
DNS servers	Vuln.	Vuln.	Vuln.	Safe	Safe	Safe
Layer-3 routing	Vuln.	Vuln.	Vuln.	Safe	Safe	Safe
DoS attacks	Vuln.	Vuln.	Vuln.	Safe	Vuln. *	Safe
DDoS attacks	Vuln.	Vuln.	Vuln.	Safe	Vuln. *	Safe
Insider attacks	Vuln.	Vuln.	Vuln.	Safe	Vuln. *	Safe
TLS cryptographic attacks	Vuln.	Safe	Safe	Safe	Safe	Safe
Harvest Now–Decrypt Later	Vuln.	Safe	Safe	Safe	Safe	Safe

5.2. The SDD-WANs Can Enable Hybrid Classical-Quantum Networks

As stated in the introduction, the US DARPA (Defense Advanced Research Projects Agency) has initiated a research program in 2023 to explore whether a hybrid Classical-Quantum network that blends classical and quantum communications can "produce a scalable, vastly more secure networking infrastructure". Prior to this paper, there is no known classical network with immunity to external cyber-attacks, which can provide "authenticated classical channels" to control of QKD networks. The SDD-WANs proposed in this paper can thus enable hybrid Classical-Quantum networks that integrate a QKD network with a classical SDD-WAN. The SDD-WAN provides the "classical authenticated channels" needed for the control of QKD networks in a programmable layer-3 network which is immune to external cyber-attacks. As shown in Table 6 above, the hybrid Classical-Quantum network is immune to all the vulnerabilities of layer-3 IP that have plagued the Consumer IoT for several decades.

5.3. The SDD-WANs Can Supplant QKD Networks in the Near-Term

Given the vulnerabilities of QOK networks, and given that the security of a hybrid Classical-Quantum network 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.

As shown in Table 6, the SDD-WANs alone offer comparable security to QKD networks in practice, as secured by the computational hardness of cracking SKC/PQC, and hence the addition of a QKD network does not really add any benefit at this time.

According to the French ANSSII, "QKD networks may find some use in a few niche applications... However, the use of state-of-the-art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long term protection of data... The cost incurred by the use of QKD should not jeopardize the fight against current threats to information systems which overwhelmingly do not exploit cryptographic weaknesses".

Several researchers have stated that the drawbacks of QKD networks shown in Table 6 may be solved in time. Reference [139] states that "more research is needed to develop a comprehensive security ecosystem". Reference [135] states that "the best that can be done at present is to integrate QKD with cryptographic schemes based on computational problems". Suppose that 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 worldwide in a cost-effective manner. 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 from the European Union

Figure 4b 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 [34–36]. These hardware testbeds used a scheduling frame with 1024 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 the theoretical expectations [33].

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 4b, let the fibers in sub-layer 3a support several optical channels operating at 800 Gbps consistent with today's Silicon Photonics transceivers. Assume sub-layer-3a transports 1-Kbyte IP packets, and that a packet transmission requires one 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 = 1 K) would have a duration of ≈10.5 μs.

Figure 7a 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 μs. The end-to-end queueing delays are all ≤2 μs. Consider the D-flows between Stockholm and Madrid; the distance is ≈3140 km. Assuming a velocity of light in fiber of 200 km/ms, the fiber latency is ≈16 ms. The queueing delay is ≈1000 times smaller than the end-to-end fiber delay, which agrees with the theory presented in [33].

Figure 7b illustrates the end-to-end delay jitter of the packets upon arrival at the D-transceiver. All packets experience a delay jitter ≤1 μs. The jitters are a small fraction of the end-to-end fiber delays in the EU network, which are measured in 10 s of milliseconds.

Figure 7c 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 = 1024 time slots). The most heavily loaded D-switch occurs at Berlin, with a steady-state size of about 103 packets. According to Figure 7d, 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 ≈4096 time slots.

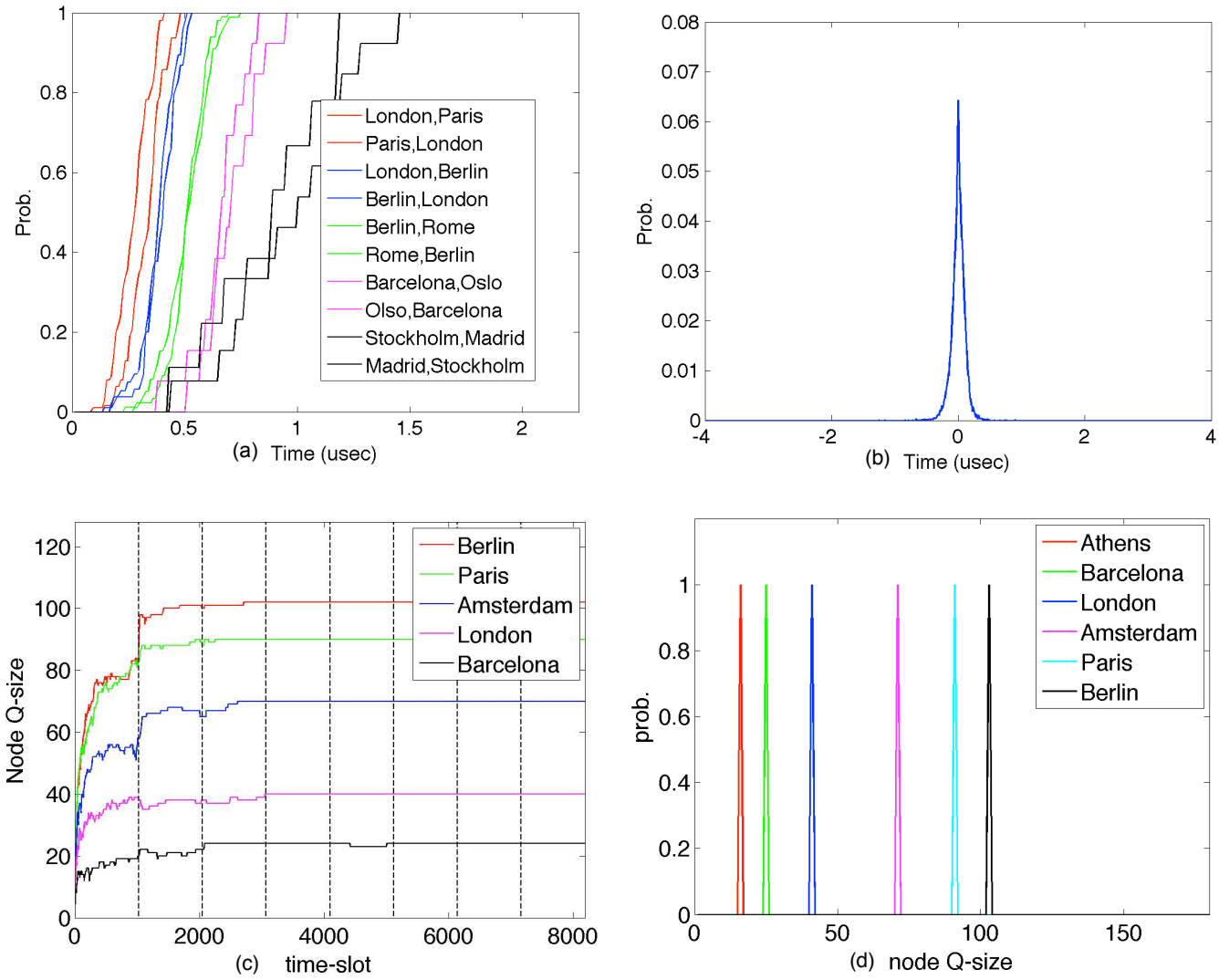


Figure 7. Performance of the SDD-WAN for the European Union: (**a**) The end-to-end delays for various D-flows across the EU are $\leq$ 2 microsec; (**b**) The delay jitter per packet, averaged over all packets and all D-flows, is $\leq$ 1 microsecond; (**c**): The evolution of the number of packets queued per D-switch (i.e., the node Q-size), versus the time-slot over 4 scheduling-frames, for several cities. The node Q-size reaches a deterministic steady-state value, after 4 scheduling-frames. (**d**): The average value of the node Q-size for several cities. The average value is $\leq$ 120 packets, in the steady-state.

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

According to Figure 7d, 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 ms. 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 of 4 would require the worst-case buffer sizes of ≈100 million packets. This rule-of-thumb illustrates a 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.

6.2. The Small Buffer-Sizing Rule for BE-IP Routers

Reference [96] presented a "small-buffer" rule-of-thumb, where the worst-case buffer size for each IoT link is $RTT \cdot C/\sqrt{N}$, and N is the number of long-living TCP flows traversing a link. Letting $N \approx 1024$, the small-buffer rule yields a worst-case buffer size of about 195 K 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 ≈780 K packets down to ≈105 packets, a reduction of ≈7400 times.

6.3. A Deterministic Buffer-Sizing Rule for D-Switches

For deterministic traffic, a new buffer-sizing rule can be stated (as first proposed in [32]). 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 [33,123]. According to prior research [33,123], the parameter K is ≈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 [33,123].

Figure 8 illustrates the evolution of the number of packets queued in each Input Port (IP), in four different D-switches in the EU network versus time. Each Input Port comprises N VOQs, and the number of packets queued in these N VOQs is called "IQ size". The horizontal axis illustrates four scheduling frames, each with 1024 time slots. The number of packets queued per IP per time slot is initially 0 and quickly increases during the first scheduling frame. By the fourth scheduling frame, the number of packets queued per IP per time slot reaches a steady-state value and remains constant. These graphs illustrate the deterministic behaviour of the queues in the D-switches. After about four scheduling-frames, a steady-state is reached, wherein the number of packets queued per IP 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 cyber-attacker (that are transmitted when no transmissions have been scheduled) will break the deterministic pattern in Figure 8. They will violate a D-schedule and will be immediately detected by the Guaranteed-IDS. Similar deterministic patterns are observed in Figures 9 and 10.

Figure 9 illustrates the evolution of the number of packets queued for each Output Port (OP), in four different D-switches in the EU network, versus time. Each Output Port is fed packets from N VOQs, and the number of packets queued in these N VOQs is called "OQ Size" The number of packets queued per OP 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 four scheduling frames, a steady state pattern is reached, wherein the number of packets queued per OP 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 10 illustrates the evolution of the size of the individual Virtual Output Queues (VOQs) in four different D-switches in the EU network versus time (only one VOQ is shown for each switch). The number of packets queued per 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 four scheduling frames, a steady state pattern is reached, wherein the number of packets queued per 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.

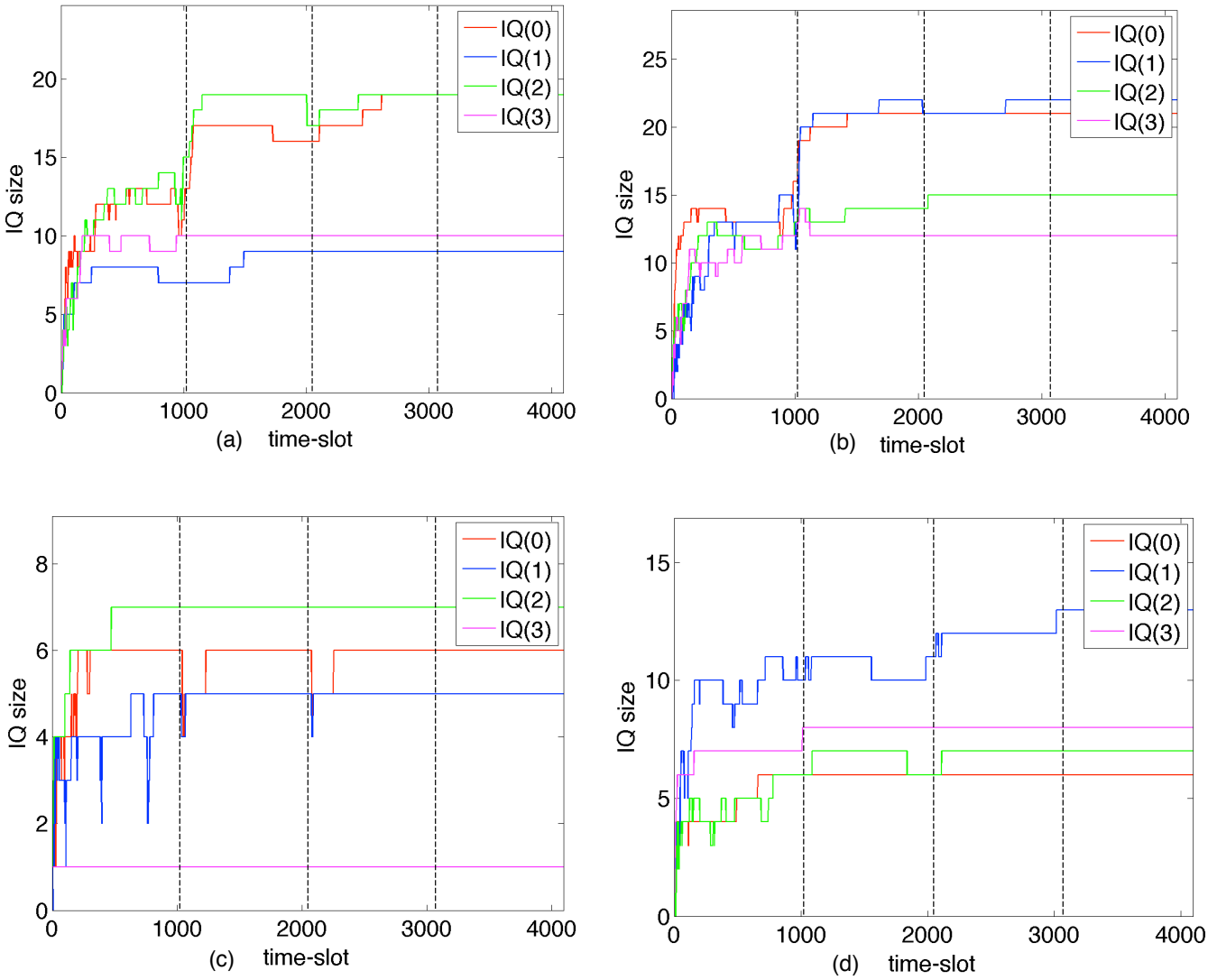


Figure 8. Evolution of the number of packets queued per Input Port (IP), for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome). (**a**) Evolution of the number of packets queued in four IPs (labelled 0…3) in the Amsterdam switch, over 4 scheduling-frames spanning 4096 time-slots. The number of packets queued per IP reaches a deterministic steady-state value, after 4 scheduling-frames. (**b**–**d**) present similar plots for the Berlin, Madrid and Rome D-switches. Each IP contains $\leq$25 queued packets on average, a very small occupancy given the %100 link utilization.

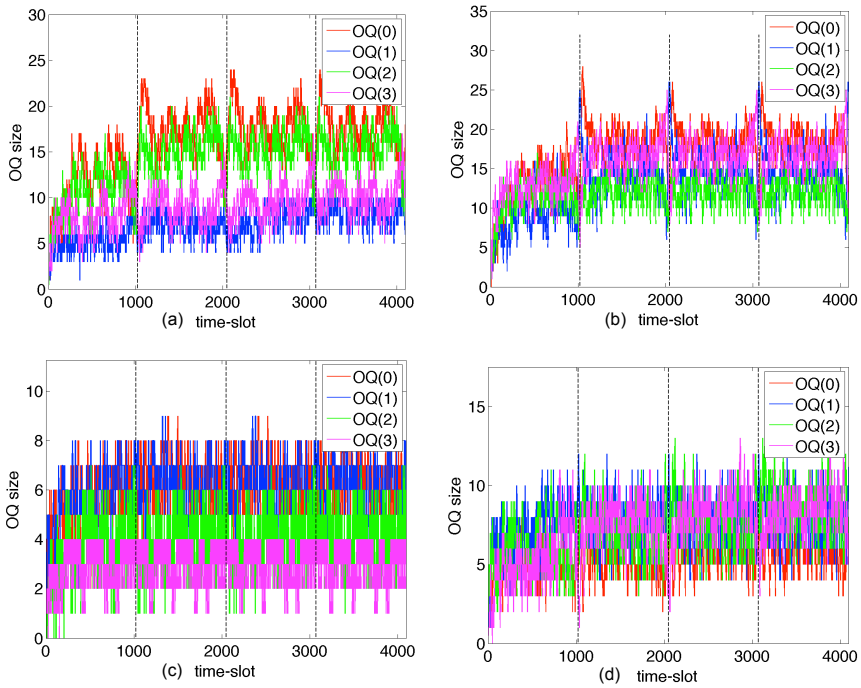


Figure 9. Evolution of the number of packets queued per Output Port (OP), for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome). (**a**) Evolution of the number of packets queued for four OPs (labelled 0...3) in the Amsterdam switch, over 4 scheduling-frames spanning 4096 time-slots. The number of packets queued per OP reaches a deterministic steady-state pattern, after 4 scheduling-frames. (**b**–**d**) present similar plots for the Berlin, Madrid and Rome D-switches. Each OP contains $\leq$25 queued packets on average, a very small occupancy given the %100 link utilization.

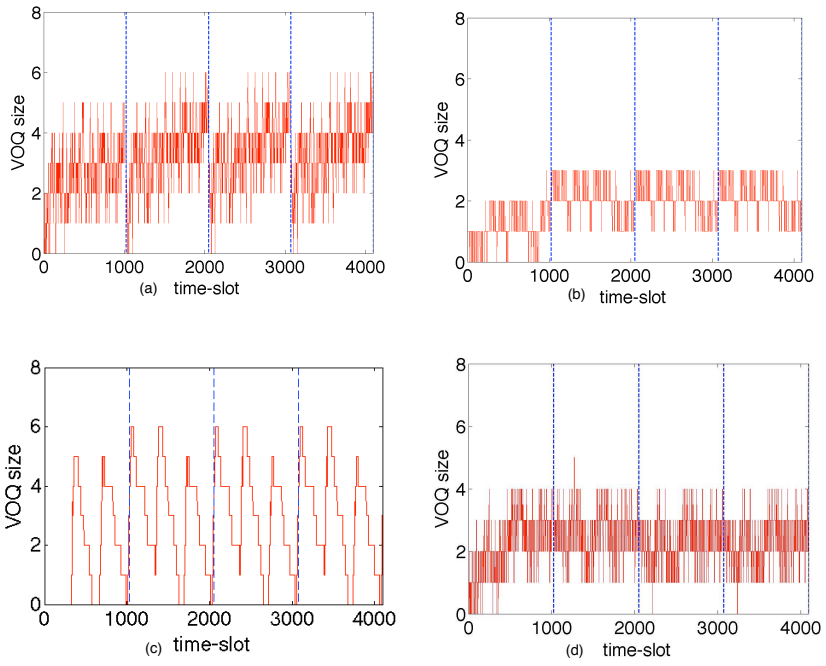


Figure 10. Evolution of the number of packets queued per VOQ for 4 D-switches in the EU SDD-WAN (Amsterdam, Berlin, Madrid, Rome). (**a**) Evolution of the number of packets queued in one VOQ in the Amsterdam switch, over 4 scheduling-frames spanning 4096 time-slots. The number of packets queued in this VOQ reaches a deterministic steady-state pattern, after 4 scheduling-frames. (**b**–**d**) present similar plots for the Berlin, Madrid and Rome D-switches. Each VOQ contains $\leq$10 queued packets on average, a very small occupancy given the %100 link utilization.

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

Table 7 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 USD 51.6 billion. About 75% of this figure represents products, while about 25% represents services. In 2022, the total global revenue is ≈USD 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 ≈USD 90 billion in 2022.

Cisco estimates that about 95% of configuration changes in layer-3 equipment (i.e., routers and firewalls) are performed manually [11,12], 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 ≈USD 225 billion annually (in 2022). The combined global capital and operational costs for layer-3 are about USD 315 billion annually in 2022.

Table 7. Revenue from 2022 annual reports.

Company	2022 Annual Revenue
Arista	USD 4.381 billion
Cisco	USD 51.6 billion
Huawei	USD 92.380 billion
Juniper	USD 5.301 billion
Nokia	USD 26.251 billion
Total	USD 179.91 billion

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) [11,12]. According to Google, layer-3 links operate at ≈25% utilization [101]. Hence, the global costs (capital and operational) due to "over-provisioning" can be estimated at 75% of the total global costs, i.e., USD 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.

Consider the SDD-WAN for the EU shown in Figure 4b 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 ≈USD 2.1 million. Each FPGA requires some extra components (i.e., transducers (i.e., electrical to optical), D-transceivers, and power supplies), costing ≈USD 150K. The total capital cost for the EU network is ≈USD 44 million, which is 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 unauthorized or malicious packet sent from any type of external cyber-attacker out of ≈119 billion transmitted packets/second. Equivalently, the FPGAs can detect even a single unauthorized/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, using deterministic electrical, wireless, or optical technologies. 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 ≈USD

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 with operational costs of ≈USD 315 billion annually, which is equal to a savings of about USD 260 billion annually. It is safe to say that the cost savings are in the range of USD 100s of billions annually.

8. Conclusions

The Consumer IoT has relied upon "best-effort" communications for four decades. It provides no guarantees that data are 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 ≈17.5 million DoS/DDoS attacks in 2024, and ≈20 million attacks in 2025. According to the US National Academy of Engineering, achieving "Security in Cyberspace" is a "Grand Challenge" problem of the 21st century [13].

This paper has explored the hardware-enforced cyber-security to address the NAE problem of "Security in Cyberspace" for critical infrastructure. It introduces a next-generation "Software-Defined-Deterministic Industrial Internet of Things" (SDD-IIoT), which can support many SDD-WANs. The SDD-IIoT utilizes a new forwarding-plane for programmable deterministic M2M traffic flows (D-flows) comprising many simple authenticated D-switches, implemented with FPGAs. The forwarding plane utilizes an "Admission-Control/Access-Control" system, to control access to network bandwidth. The AC/AC system utilizes many collaborative AI-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.

Kleinrock proposed the traditional "narrow waist" model of the Consumer IoT three decades ago in 1994, which has not changed much since then. 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 bypasses IP, and thus eliminates several cyber-security vulnerabilities that have existed in layer-3 of the Consumer IoT for many decades. It implements "Authenticated Encrypted Deterministic Channels" directly in hardware (in sub-layer-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 sub-layer-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 USD 100s of billions per year in reduced capital, energy, and operational costs.
(4) It can reduce the global costs of cyber-crime to society, estimated to exceed USD 10 trillion per year in 2025. If the global costs of cyber-crime can be reduced by a modest 25%, the savings potentially exceed USD 2.5 trillion per year.

(5) It can support the Metaverse by providing large increases in layer-3 capacity and security, while decreasing the capital and operational costs by USD 100s of billions per year.
(6) In practice, the SDD-WANs can have comparable security to QKD networks, as determined by the computational hardness of cracking SKC/PKC. The SDD-WANs thus provide a classical network with exceptionally strong cyber-security.
(7) The SDD-WANs can enable hybrid Classical-Quantum networks by integrating a QKD network with a programmable SDD-WAN that provides "authenticated classical channels" and immunity 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 Zero Trust Architectures, the number of internal cyber-attacks can also be significantly reduced or eliminated.
(8) According to the US "National Security Agency", QKD networks have several vulnerabilities, i.e., they 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 of these vulnerabilities, three national security agencies representing thousands of cyber-security experts (the American NSA, the British NSCS, and French ANSSI) agree that QKD networks should not be recommended at this time. In practice, SDD-WANs can have comparable security to QKD networks, as 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 future time when QKD networks are ready to be deployed on a large-scale to millions/billions of users worldwide in a cost-effective manner.

Funding: This research was performed as part of the author's consulting practice and was funded through the author's consulting practice.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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.

Acknowledgments: The author would like to thank the Paolo Maistri for organizing a special issue on hardware security and trust. I would like to thank the reviewers for their comments, which helped to focus the paper. The reviews and comments are greatly appreciated. I would like to thank the editors for their work, Madalina Handrea, Vlad Ursulescu, Afra Wang and Krzysztof Szczypiorski.

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 briefly summarizes the most common abbreviations used in this paper.

Table A1. Commonly used abbreviations.

Abbreviation	Description
AE	Authenticated Encryption
AEDC	Authenticated and Encrypted Deterministic Channel (i.e., a D-flow)
AES	Advanced Encryption Standard (a cipher)
BE	Best Effort
BE-IP, BE-flow	Best-Effort Internet Protocol, Best-Effort Traffic Flow
BE-VPN	Best-Effort "Virtual Private Network" (in the Consumer IoT)
BGP	"Border Gateway Routing Protocol" (to Route Packets)

Table A1. *Cont.*

Abbreviation	Description
BSD	"Berkeley Sockets Distribution" Software (to Program "Sockets")
C-IoT	Consumer IoT
D, D-flow,	Deterministic, Deterministic Traffic Flow (i.e., AEDC)
D-switch, D-IIoT	Deterministic Packet Switch, Deterministic Industrial IoT
D-Schedule	a "Gine-Grain" Deterministic Periodic Schedule, to Control a D-Switch
DetNet	"Deterministic Networking" Group in the IETF
DetNet Converged WAN	Converged WAN Network (Proposed by the DetNet Group of the IETF)
D-VPN	Deterministic Virtual Private Network
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 ([42])
ULL	Ultra-Low Latency
ZTA	Zero Trust Architecture

Table A2 briefly summarizes 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	Overloads 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	Modifies IP packet headers to masquerade as a trusted peer	—- Effectively eliminated —— SDD-IIoT does not use IP (or IP packet headers)
Phishing attack	Provides malicious email or link to malicious website	—- Effectively eliminated—- Links to malicious websites will not be pre-approved
Spear phishing attacks	Personalizes contact to individual; provides malicious email; or links to malicious website	—- Effectively eliminated—- links to malicious websites will not be pre-approved
Man-in-the-Middle (MITM) attack	Cyber-attacker is interposed between two communicating entities by spoofing	—- Effectively eliminated —— spoofing attacks eliminated (IP is not used)

Table A2. *Cont.*

Threat/Attack Name	Type of Threat/Attack in Consumer IoT	Type of Threat/Attack in SDD-IIoT
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, M.A.; Shariatmadari, H.; Singh, B. 5G URLLC: Design Challenges and System Concepts. In Proceedings of the 2018 15th International Symposium on Wireless Communication Systems (ISWCS), Lisbon, Portugal, 28–31 August 2018; pp. 1–6.
2. Pokhrel, S.R.; Ding, J.; Park, J.; Park, O.S.; Choi, J. Towards Enabling Critical mMTC: A Review of URLLC within mMTC. *IEEE Access* **2020**, *8*, 131796–131813. [CrossRef]
3. Park, J.; Samarakoon, S.; Shiri, H.; Abdel-Aziz, M.K.; Nishio, T.; Elgabli, A.; Bennis, M. Extreme Ultra-Reliable and Low-Latency Communication. *Nat. Electron.* **2022**, *5*, 133–141. [CrossRef]
4. Gevros, P.; Crowcroft, J.; Kirstein, P.; Bhatti, S. Congestion Control Mechanisms and the Best Effort Service Model. *IEEE Netw.* **2001**, *15*, 16–26. [CrossRef]
5. Lefelhocz, C.; Lyles, B.; Shenker, S.; Zhang, L. Congestion Control for Best-Effort Service: Why we need a New Paradigm. *IEEE Netw.* **1996**, *10*, 10–19. [CrossRef]
6. Afanasyev, A.; Tilly, N.; Reiher, P.; Kleinrock, L. Host-to-Host Congestion Control for TCP. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 304–342. [CrossRef]
7. Gettys, J.; Nichols, K. BufferBloat: Dark Buffers in the Internet. *ACM Queue* **2011**, *9*, 40–54. [CrossRef]
8. Butler, K.; Farley, T.R.; McDaniel, P.; Rexford, J. A Survey of BGP Security Issues and Solutions. *Proc. IEEE* **2009**, *98*, 100–122. [CrossRef]
9. Goldberg, S. Why is it Taking So Long to Secure Internet Routing? *Commun. ACM* **2014**, *57*, 56–63. [CrossRef]
10. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
11. CISCO. Cisco Annual Internet Report (2018–2023). Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 7 March 2024).
12. CISCO. Global—2021 Forecast Highlights. Available online: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf (accessed on 7 March 2024).
13. US National Academy of Engineering. NAE Grand Challenges for Engineering: Secure Cyberspace. Available online: https://www.engineeringchallenges.org/challenges/cyberspace.aspx (accessed on 7 March 2024).
14. Butun, I.; Osterberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
15. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges, Elsevier. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
16. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
17. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
18. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
19. Xin, Y.; Kong, L.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
20. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
21. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
22. Demertzi, V.; Demertzis, S.; Demertzis, K. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Appl. Sci.* **2023**, *13*, 790. [CrossRef]

23. de Azambuja, A.J.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics* **2023**, *12*, 1920. [CrossRef]
24. US NSA (National Security Agency). Quantum Computing and Post Quantum Cryptography, FAQs (Frequently Asked Questions), Document PP-21-1120, 4 August 2021. Available online: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (accessed on 7 March 2024).
25. US NSA (National Security Agency). Quantum Key Distribution (QKD) and Quantum Cryptography (QC). Available online: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (accessed on 10 March 2024).
26. US CISA (Cybersecurity and Infrastructure Security Agency). *Critical Infrastructure Security and Resilience*; USA CISA: Arlington, VA, USA, 2023. Available online: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience (accessed on 8 March 2024).
27. NATO, EU-NATO Task Force on the Resilience of Critical Infrastructure, Final Assessment Report. Available online: https://commission.europa.eu/system/files/2023-06/EU-NATO_Final
28. Tehranipoor, M.; Wang, C. (Eds.) *Introduction to Hardware Security and Trust*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011.
29. Maistri, P. Countermeasures against Fault Attacks: The Good, the Bad, and the Ugly. In Proceedings of the 2011 IEEE 17th International On-Line Testing Symposium, Athens, Greece, 13–15 July 2011; pp. 134–137.
30. Jin, Y. Introduction to Hardware Security. *Electronics* **2015**, *4*, 763. [CrossRef]
31. Alioto, M. Trends in Hardware Security: From Basics to ASICs. *IEEE Solid-State Circuits Mag.* **2019**, *11*, 56–74. [CrossRef]
32. Szymanski, T.H. The Cyber Security via Determinism Paradigm for a Quantum Safe Zero Trust Deterministic Internet of Things (IoT). *IEEE Access* **2022**, *10*, 45893–45930. [CrossRef]
33. Szymanski, T.H. An Ultra Low Latency Guaranteed-Rate Internet for Cloud Services. *IEEE Trans. Netw.* **2014**, *24*, 123–136. [CrossRef]
34. Szymanski, T.H. Supporting Consumer Services in a Deterministic Industrial Internet Core Network. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
35. Szymanski, T.H. Securing the Industrial-Tactile Internet of Things with Deterministic Silicon Photonic Switches. *IEEE Access* **2016**, *4*, 8236–8249. [CrossRef]
36. Szymanski, T.H. Security and Privacy for a Green Internet of Things. *IEEE IT Prof.* **2017**, *19*, 34–41. [CrossRef]
37. Wang, L.J.; Zhang, K.Y.; Wang, J.Y.; Cheng, J.; Yang, Y.H.; Tang, S.B.; Yan, D.; Tang, Y.L.; Liu, Z.; Yu, Y.; et al. Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography. *NPJ Quantum Inf.* **2021**, *7*, 67. [CrossRef]
38. Kleinrock, L.; National Research Council; NRENAISSANCE Committee. *Realizing the Internet Future: The Internet and Beyond*; National Academy Press: Washington, DC, USA, 1994.
39. Popa, L.; Ghodsi, A.; Stoica, I. HTTP as the Narrow Waist of the Future Internet. In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Monterey, CA, USA, 20–21 October 2010; pp. 1–6.
40. Akhshabi, S.; Dovrolis, C. The Evolution of Layered Protocol Stacks leads to an Hourglass-Shaped Architecture. In Proceedings of the ACM SIGCOMM 2011 Conference, Toronto, ON, Canada, 15–19 August 2011; pp. 206–217.
41. Beck, M. On the Hourglass Model. *Commun. ACM* **2019**, *62*, 48–57. [CrossRef]
42. Rescorla, E. *IETF (Internet Engineering Task Force) RFC (Request for Comments) 8446, The Transport Layer Security (TLS) Protocol Version 1.3*; 2018; pp. 1–160. Available online: https://datatracker.ietf.org/doc/html/rfc8446 (accessed on 8 March 2024).
43. Douligeris, C.; Mitrokotsa, A. DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. *Comput. Netw.* **2004**, *44*, 643–666. [CrossRef]
44. Yan Q., Yu FR., Yan, Q.; Yu, F.R. Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing. *IEEE Commun. Mag.* **2015**, *53*, 52–59. [CrossRef]
45. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. *Comput. Commun.* **2017**, *107*, 30–48. [CrossRef]
46. Zlomislić, V.; Fertalj, K.; Sruk, V. Denial of Service Attacks, Defences and Research Challenges. *Clust. Comput.* **2017**, *20*, 661–671. [CrossRef]
47. Bawany, N.Z.; Shamsi, J.A.; Salah, K. DDoS Attack Detection and Mitigation using SDN: Methods, Practices, and Solutions. *Arab. J. Sci. Eng.* **2017**, *42*, 425–441. [CrossRef]
48. Praseed, A.; Thilagam, P.S. DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 661–685. [CrossRef]
49. Osterweil, E.; Stavrou, A.; Zhang, L. 21 Years of Distributed Denial-of-Service: A Call to Action. *IEEE Comput.* **2020**, *53*, 94–99. [CrossRef]
50. Vishwakarma, R.; Jain, A.K. A Survey of DDoS Attacking Techniques and Defence Mechanisms in the IoT Network. *Telecommun. Syst.* **2020**, *73*, 3–25. [CrossRef]
51. Eliyan, L.F.; Di Pietro, R. DoS and DDoS Attacks in Software Defined Networks: A Survey of Existing Solutions and Research Challenges. *Future Gener. Comput. Syst.* **2021**, *122*, 149–171. [CrossRef]
52. Bhargavan, K.; Fournet, C.; Kohlweiss, M.; Pironti, A.; Strub, P.Y. Implementing TLS with Verified Cryptographic Security. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 445–459.

53. Bürstinghaus-Steinbach, K.; Krauß, C.; Niederhagen, R.; Schneider, M. Post-quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and Sphincs+ with mbed tTLS. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, 5–9 October 2020; pp. 841–852.
54. Mell, P.; Marks, D.; McLarnon, M. A Denial-of-Service Resistant Intrusion Detection Architecture. *Comput. Netw.* **2000**, *34*, 641–658. [CrossRef]
55. Jager, T.; Kohlar, F.; Schäge, S.; Schwenk, J. On the Security of TLS-DHE in the Standard Model. In *Advances in Cryptology—CRYPTO 2012, Proceedings of the 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 273–293.
56. Krawczyk, H.; Paterson, K.G.; Wee, H. On the Security of the TLS Protocol: A Systematic Analysis. In *Advances in Cryptology—CRYPTO 2013, Proceedings of the 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 429–448.
57. Eldewahi, A.E.; Sharfi, T.M.; Mansor, A.A.; Mohamed, N.A.; Alwahbani, S.M. SSL/TLS Attacks: Analysis and Evaluation. In Proceedings of the 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), Khartoum, Sudan, 7–9 September 2015; pp. 203–208.
58. Sirohi, P.; Agarwal, A.; Tyagi, S. A Comprehensive Study on Security Attacks on SSL/TLS Protocol. In Proceedings of the 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 14–16 October 2016; pp. 893–898.
59. Waked, L.; Mannan, M.; Youssef, A. The Sorry State of TLS Security in Enterprise Interception Appliances. *Digit. Threat. Res. Pract.* **2020**, *1*, 1–26. [CrossRef]
60. Paracha, M.T.; Dubois, D.J.; Vallina-Rodriguez, N.; Choffnes, D. IoTLS: Understanding TLS Usage in Consumer IoT Devices. In Proceedings of the 21st ACM Internet Measurement Conference, New York, NY, USA, 2–4 November 2021; pp. 165–178.
61. Meyer, C.; Schwenk, J. SoK: Lessons Learned from SSL/TLS Attacks. In *International Workshop on Information Security Applications*; Springer International Publishing: Cham, Switzerland, 2013; pp. 189–209.
62. Sandhu, R.; Ferraiolo, D.; Kuhn, R. The NIST Model for Role-Based Access Control: Towards a Unified Standard. In Proceedings of the ACM Workshop Role-Based Access Control, Berlin, Germany, 26–27 July 2000; Volume 10, pp. 344287–344301.
63. Kuhn, D.R.; Coyne, E.J.; Weil, T.R. Adding Attributes to Role-Based Access Control. *IEEE Comput.* **2010**, *43*, 79–81. [CrossRef]
64. Hu, V.C.; Ferraiolo, D.; Kuhn, R.; Friedman, A.R.; Lang, A.J.; Cogdell, M.M.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft). *NIST Spec. Publ.* **2013**, *800*, 1–54.
65. Hu, V.C.; Kuhn, D.R.; Ferraiolo, D.F.; Voas, J. Attribute-Based Access Control. *IEEE Comput.* **2015**, *16*, 85–88. [CrossRef]
66. The White House. *Executive Order on Improving the Nation's Cybersecurity*; The White House: Washington, DC, USA, 2021. Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed on 8 March 2024).
67. US NIST (National Institute of Standards and Technology). Zero Trust Architecture, Publication SP-800-207. *August 2020*. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed on 7 March 2024).
68. Kerman, A.; Scarfone, K.; Symington, S.; Barker, W. *Implementing a Zero Trust Architecture*; NIST (National Institute of Standards and Technology): Gaithersburg, MD, USA, 2022. Available online: https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf (accessed on 8 March 2024).
69. Bace, R.; Mell, P.; NIST Special Publication on Intrusion Detection Systems. 1 November 2001. Available online: https://www.nist.gov/publications/intrusion-detection-systems (accessed on 7 March 2024).
70. Scarfone, K.; Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94. 2007; pp. 1–127. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf (accessed on 7 March 2024).
71. Mukherjee, B.; Heberlein, T.D.; Levitt, K.N. Network Intrusion Detection. *IEEE Netw.* **1994**, *8*, 26–41. [CrossRef]
72. Debar, H.; Dacier, M.; Wespi, A. Towards a Taxonomy of Intrusion-Detection Systems. *Comput. Netw.* **1999**, *31*, 805–822. [CrossRef]
73. Hubballi, N.; Suryanarayanan, V. False Alarm Minimization Techniques in Signature-Based Intrusion Detection Systems: A Survey. *Comput. Commun.* **2014**, *49*, 1–17. [CrossRef]
74. Masdari, M.; Khezri, H. A Survey and Taxonomy of the Fuzzy Signature-based Intrusion Detection Systems. *Appl. Soft Comput.* **2020**, *92*, 106301. [CrossRef]
75. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Macia-Fernandez, G.; Vazquez, E. Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
76. Jyothsna, V.; Prasad, R.; Prasad, K.M. A Review of Anomaly Based Intrusion Detection Systems. *Int. J. Comput. Appl.* **2011**, *28*, 26–35. [CrossRef]
77. Javaid, A.; Niyaz, Q.; Sun, W.; Alam, M. A Deep Learning Approach for Network Intrusion Detection System. In Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS), New York, NY, USA, 24 May 2016; Volume 3, p. 2.
78. Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
79. Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, Q. A Deep Learning Approach to Network Intrusion Detection. *IEEE Trans. Emerg. Top. Comp. Intell.* **2018**, *2*, 41–50. [CrossRef]

80. Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* **2019**, *7*, 41525–41550. [CrossRef]
81. US NIST (National Institute of Standards and Technology). Federal Information Processing Standards (FIPS), Publication 197, Announcing the Advanced Encryption Standard (AES). 26 November 2001. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf (accessed on 7 March 2024).
82. Daemen, J.; Rijmen, V. *The Design of Rijndael*; Springer: New York, NY, USA, 2002.
83. Nir, Y.; Langley, A. *Chacha20 and Poly1305 for IETF Protocols*; IETF (Internet Engineering Task Force) RFC 8439; 2018; pp. 1–46. Available online: https://datatracker.ietf.org/doc/rfc8439/ (accessed on 8 March 2024).
84. Grover, L.K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]
85. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
86. McGrew, D. *An Interface and Algorithms for Authenticated Encryption*; IETF (Internet Engineering Task Force), RFC 5116; 2008. Available online: https://datatracker.ietf.org/doc/html/rfc5116/ (accessed on 8 March 2024).
87. Perlner, R.A.; Cooper, D.A. Quantum Resistant Public Key Cryptography: A Survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet, Gaithersburg, MD, USA, 14–16 April 2009; pp. 85–93.
88. Chen, L.; Jordan, S.; Liu, Y.K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D. Report on Post-Quantum Cryptography. US NIST Interagency/Internal Report (NISTIR)—8105. April 2016. Volume 12, 10 pages. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf (accessed on 8 March 2024).
89. ETSI (European Telecommunications Standards Institute). Quantum Safe Public Key Encryption and Key Encapsulation; ETSI TR 103 823 v1.1.2; Technical Report; October 2021. Available online: https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.01_60/tr_103823v010101p.pdf (accessed on 8 March 2024).
90. ETSI (European Telecommunications Standards Institute). Quantum Safe Virtual Private Networks; ETSI TR 103 617 v1.1.1; Technical Report; August 2018. Available online: https://www.etsi.org/deliver/etsi_tr/103600_103699/103617/01.01.01_60/tr_103617v010101p.pdf (accessed on 8 March 2024).
91. Xiao, X.; Ni, L.M. Internet QoS: A Big Picture. *IEEE Netw.* **1999**, *13*, 8–18. [CrossRef]
92. Nong, G.; Hamdi, M. On the Provision of Quality-of-Service Guarantees for Input Queued Switches. *IEEE Commun. Mag.* **2000**, *38*, 62–69.
93. Meddeb, A. Internet QoS: Pieces of the Puzzle. *IEEE Commun. Mag.* **2010**, *48*, 86–94. [CrossRef]
94. Parekh, A.K.; Gallager, R.G. A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Single-Node Case. *IEEE/ACM Trans. Netw.* **1993**, *1*, 344–357. [CrossRef]
95. Parekh, A.K.; Gallager, R.G. A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Multiple Node Case. *IEEE/ACM Trans. Netw.* **1994**, *2*, 137–150. [CrossRef]
96. Appenzeller, G.; Keslassy, I.; McKeown, N. Sizing Router Buffers. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 281–292. [CrossRef]
97. Iyer, S.; Kompella, R.R.; Mckeown, N. Designing Packet Buffers for Router Linecards. *IEEE Trans. Netw.* **2008**, *16*, 705–717. [CrossRef]
98. Anantharam, V.; McKeown, N.; Mekittikul, A.; Walrand, J. Achieving 100% Throughput in an Input Queued Switch. *IEEE Trans. Commun.* **1999**, *47*, 1260–1267.
99. Mckeown, N. The iSLIP Scheduling Algorithm for Input-Queued Switches. *IEEE/ACM Trans. Netw.* **1999**, *7*, 188–201. [CrossRef]
100. Odlyzko, A. Data Networks are Lightly Utilized, and Will Stay That Way. *Rev. Netw. Econ.* **2003**, *2*. [CrossRef]
101. Hassidim, A.; Raz, D.; Segalov, M.; Shaqed, A. Network Utilization: The Flow View. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 1429–1437.
102. Braken, R.; Clark, D.; Shenker, S. *Integrated Services in the Internet Architecture—An Overview*; IETF (Internet Engineering Task Force) RFC 1633; 1994. Available online: https://datatracker.ietf.org/doc/html/rfc1633 (accessed on 8 March 2024).
103. Black, D.; Jones, P. *Differentiated Services (DiffServ) and Real-Time Communications*; IETF (Internet Engineering Task Force) RFC 7657; 2015. Available online: https://datatracker.ietf.org/doc/html/rfc7657 (accessed on 8 March 2024).
104. IEEE 802.org. Deterministic Ethernet: 802.1 Standards for Real-Time Process Control, Industrial Automation, and Vehicular Networks. 2012. Available online: https://www.ieee802.org/802_tutorials/2012-11/8021-tutorial-final-v4.pdf (accessed on 8 March 2024).
105. Hermeto, R.T.; Gallais, A.; Theoleyre, F. Scheduling for IEEE-802.15.4-TSCH and Slow Channel Hopping MAC in Low Power Industrial Wireless Networks: A Survey. *Comput. Commun.* **2017**, *114*, 84–105. [CrossRef]
106. Dujovne, D.; Watteyne, T.; Vilajosana, X.; Thubert, P. 6TiSCH: Deterministic IP-enabled Industrial Internet (of Things). *IEEE Commun. Mag.* **2014**, *52*, 36–41. [CrossRef]
107. Finn, N.; Thubert, P. *Deterministic Networking Problem Statement (09)*; IETF Internet-Draft, Standards Track; December 2018; pp. 1–20. Available online: https://datatracker.ietf.org/doc/html/draft-ietf-detnet-problem-statement (accessed on 8 March 2024).
108. Grossman, E. *Deterministic Networking Use Cases*; IETF (Internet Engineering Task Force)draft; May 2019. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc8578.txt.pdf (accessed on 8 March 2024).

109. Finn, N.; Thubert, P.; Varga, B.; Farkas, J. *Deterministic Networking Architecture*; IETF (Internet Engineering Task Force) Internet RFC 8655; 2019. Available online: https://datatracker.ietf.org/doc/rfc8655/ (accessed on 8 March 2024).
110. Liu, B.; Ren, S.; Wang, C.; Angilella, V.; Medagliani, P.; Martin, S.; Leguay, J. Towards Large-Scale Deterministic IP Networks. In Proceedings of the 2021 IFIP Networking Conference (IFIP Networking), Espoo and Helsinki, Finland, 21–24 June 2021; pp. 1–9.
111. Singla, A.; Chandrasekaran, B.; Godfrey, P.B.; Maggs, B. The Internet at the Speed of Light. In Proceedings of the 13th ACM Workshop on Hot Topics in Networks, Los Angeles, CA, USA, 27–28 October 2014; pp. 1–7.
112. Fettweis, G.; Boche, H.; Wiegand, T.; Zielinski, E.; Schotten, H.; Merz, P.; Hirche, S.; Festag, A.; Häffner, W.; Meyer, M.; et al. *The Tactile Internet, ITU-T Technology Watch Report*; ITU: Geneva, Switzerland, 2014; pp. 1–24. Available online: https://www.itu.int/dms_pub/itu-t/opb/gen/T-GEN-TWATCH-2014-1-PDF-E.pdf (accessed on 8 March 2024).
113. Nasrallah, A.; Thyagaturu, A.S.; 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 Commun. Surv. Tutor.* **2018**, *21*, 88–145. [CrossRef]
114. Chen, W.J.; Chang, C.S.; Huang, H.Y. Birkoff-von Neumann Input Buffered Crossbar Switches for Guaranteed-Rate Services. *IEEE Trans. Commun.* **2001**, *49*, 1145–1147.
115. Chang, C.S.; Lee, D.S.; Yue, C.Y. Providing Guaranteed Rate Services in the Load Balanced Birkhoff-von Neumann Switches. *IEEE/ACM Trans. Netw.* **2008**, *14*, 644–656. [CrossRef]
116. Koksal, C.E.; Gallager, R.G.; Rohrs, C.E. Rate Quantization and Service Quality over Single Crossbar Switches. In Proceedings of the IEEE INFOCOM 2004, Hong Kong, China, 7–11 March 2004; Volume 3, pp. 1962–1973.
117. Keslassy, I.; Kodialam, M.; Lakshman, T.V.; Stilliadis, D. On Guaranteed Smooth Scheduling for Input-Queued Switches. *IEEE/ACM Trans. Netw.* **2005**, *13*, 1364–1375. [CrossRef]
118. Mohanty, S.R.; Bhuyan, L.N. Guaranteed Smooth Switch Scheduling with Low Complexity. In Proceedings of the GLOBECOM'05, IEEE Global Telecommunications Conference, St. Louis, MO, USA, 28 November–2 December 2005; Volume 1, p. 5.
119. Szymanski, T.H. A Low Jitter Guaranteed Rate Scheduling Algorithm for Packet Switched IP Routers. *IEEE Trans. Commun.* **2009**, *57*, 3446–3459. [CrossRef]
120. Szymanski, T.H.; Gilbert, D. Internet multicasting of IPTV with essentially-zero delay jitter. *IEEE Trans. Broadcast.* **2009**, *55*, 20–30. [CrossRef]
121. Szymanski, T.H.; Gilbert, D. Provisioning Mission-Critical Telerobotic Control Systems over Internet backbone Networks with Essentially-Perfect QoS. *IEEE J. Sel. Areas Commun.* **2010**, *28*, 630–643. [CrossRef]
122. Szymanski, T.H. Max-Flow Min-Cost Routing in a Future Internet with Improved QoS Guarantees. *IEEE Trans. Commun.* **2013**, *61*, 1485–1497. [CrossRef]
123. Szymanski, T.H. Method to Achieve Bounded Buffer Sizes and Quality of Service Guarantees in the Internet Network. US Patent 8,665,722 B2, 4 March 2014.
124. Szymanski, T.H. Method to Achieve Bounded Buffer Sizes and Quality of Service Guarantees in the Internet Network. US Patent 9,584,431 B2, 28 February 2017.
125. Szymanski, T.H. Reduced-Complexity Integrated Guaranteed-Rate Optical Packet Switch. US Patent 10,687,128 B2, 16 June 2020.
126. Szymanski, T.H. Methods to Strengthen Cyber-Security and Privacy in a Deterministic Internet of Things. US Patent 11,019,038 B2, 25 May 2021.
127. Kaufman, C.; Hoffman, P.; Nir, Y.; Eronen, P.; Kivinen, T. *Internet Key Exchange Protocol Version 2 (IKEV2)*; IETF (Internet Engineering Task Force) RFC 7296; 2014; pp. 1–138. Available online: https://datatracker.ietf.org/doc/html/rfc7296 (accessed on 8 March 2024).
128. Fluhrer, S.; Kampanakis, P.; McGrew, D.; Smyslov, V. *Mixing Preshared Keys in IKEV2 for Post Quantum Security*; IETF (Internet Engineering Task Force) RFC 8774; 2020; pp. 1–20. Available online: https://datatracker.ietf.org/doc/html/rfc8784 (accessed on 8 March 2024).
129. Bos, J.W.; Costello, C.; Naehrig, M.; Stebila, D. Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 553–570.
130. Karakus, M.; Durresi, A. A Survey: Control Plane Scalability Issues and Approaches in Software-Defined Networking (SDN). *Comput. Netw.* **2017**, *12*, 279–293. [CrossRef]
131. Bannour, F.; Souihi, S.; Mellouk, A. Distributed SDN Control: Survey, Taxonomy, and Challenges. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 333–354. [CrossRef]
132. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical Challenges in Quantum Key Distribution. *NPJ Quantum Inf.* **2016**, *2*, 1–12. [CrossRef]
133. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 839–894. [CrossRef]
134. Tsai, C.W.; Yang, C.W.; Lin, J.; Chang, Y.C.; Chang, R.S. Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. *Appl. Sci.* **2021**, *11*, 3767. [CrossRef]
135. Lella, E.; Schmid, G. On the Security of Quantum Key Distribution Networks. *Cryptography* **2023**, *7*, 53. [CrossRef]
136. Mehic, M.; Niemiec, M.; Rass, S.; Ma, J.; Peev, M.; Aguado, A.; Martin, V.; Schauer, S.; Poppe, A.; Pacher, C.; et al. Quantum Key Distribution: A Networking Perspective. *ACM Comput. Surv.* **2020**, *53*, 1–41. [CrossRef]

137. James, P.; Laschet, S.; Ramacher, S.; Torresetti, L. Key Management Systems for Large-Scale Quantum Key Distribution Networks. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento Italy, 29 August–1 September 2023; pp. 1–9.
138. *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): Sophia-Antipolis, France, 2020. Available online: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf (accessed on 8 March 2024).
139. Green, A.; Lawrence, J.; Siopsis, G.; Peters, N.A.; Passian, A. Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams. *Sensors* **2023**, *23*, 9818. [CrossRef]