Security and Privacy for a Green Internet of Things

Ted H. Szymanski, *Department of Electrical and Computer Engineering, McMaster University, Canada*

In the 21st century, the Internet of Things (IoT) will control critical infrastructure such as smart cities and the smart power grid. The author proposes a new approach to achieve exceptional performance, cybersecurity, and privacy in a green Industrial and Tactile IoT.

The Internet of Things (IoT) will control the critical infrastructure of the 21st century, including smart cities, smart manufacturing, the smart power grid, and smart transportation systems. These smart cyber-physical systems will interconnect billions of smart devices with IoT control systems, thus requiring an IoT with exceptionally low latencies and exceptionally high cybersecurity. The US National Academy of Engineering recently identified 14 grand challenges for the 21st century, including achieving cybersecurity for the IoT (bit.ly/1UObLEq). Fundamentally new approaches to achieving cybersecurity, privacy, and trust in the IoT are needed that go well beyond current approaches.

Figure 1a illustrates the US electrical power grid, which includes 7,000 power plants and about 3 million miles of transmission lines. Figure 1b shows the US oil and gas pipeline network, which includes about half a million miles of oil and gas pipelines. The cyber-physical control systems for these critical resources will include millions of smart sensors and actuators reporting to an IoT control center potentially thousands of miles away. A cyberattack against these infrastructures could have catastrophic consequences. IoT control systems must therefore support ultra-low latencies, ultra-low packet loss rates, and exceptionally strong cybersecurity and privacy.

Published by the IEEE Computer Society

1520-9202/17/$33.00 © 2017 IEEE

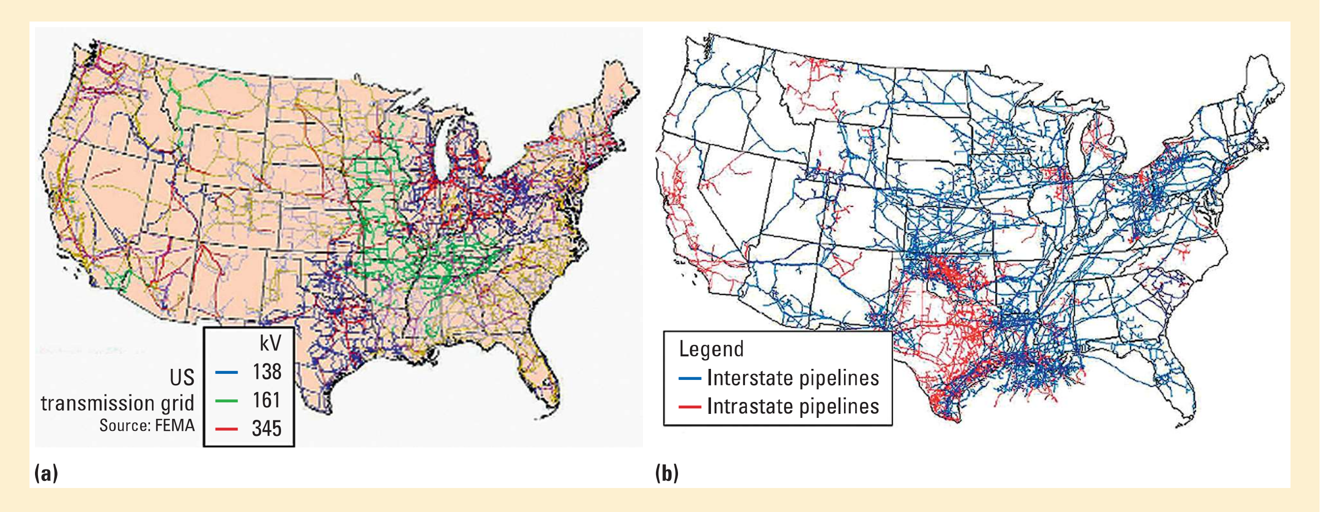

Figure 1. Critical infrastructure networks that are subject to cyberattacks. Such networks include (a) the US electricity transmission grid and (b) the US oil and gas pipeline network.

Unfortunately, today's best-effort IoT (BE-IoT) suffers from severe weaknesses. For example, it has no inherent admission control or rate control for billions of IoT users. Any user can send data at any rate to any destination at any time. Consequently, the BE-IoT suffers from frequent congestion, excessive delays, excessive packet loss, and poor energy efficiency. Delays approaching hundreds of milliseconds occur often, and denial-of-service (DoS) attacks are easy to create. The BE-IoT also offers no guarantees that data will be delivered within a strict delay deadline, or at all. According to General Electric, the future IoT could control roughly US$82 trillion in global GDP by 2030.[1] According to Juniper Research, DoS and cyberattacks could cost global industries more than $2 trillion by the year 2020.

Several international efforts are exploring ways to improve the BE-IoT to support machine-to-machine and device-to-device communications. The Industrial Internet Consortium (IIC) consists of more than 250 companies and is developing a new Industrial Internet to interconnect smart factories and industrial machines.[2] The IEEE and ITU are developing a new Tactile Internet with very low latencies for human-to-machine communications.[3,4] Neither effort has considered deterministic communications, which can be inherently NP-hard. A unified, ultra-low-latency IoT network could be called the Industrial and Tactile IoT, and new approaches to achieving improved security and privacy in this Industrial-Tactile IoT are required.[5]

Here, a new approach to achieving exceptional security and privacy in the IoT is explored. The combination of a centralized control plane using software-defined networking (SDN) technologies, the use of deterministic virtual networks (DVNs), and lightweight encryption with long keys in layer 2 can offer significant benefits.

Advantages of Deterministic Virtual Networks

A deterministic system is a system in which all events are predetermined—that is, there is no randomness. In a deterministic network, the relative times for authorized packet transmissions in a periodic scheduling frame can be predetermined for every link, and they will never deviate from these predetermined relative times. This unique combination therefore offers a new dimension for improved security and privacy that has not been previously explored.

Deterministic communications will introduce some NP-hard routing and scheduling problems.[6] However, these complexities can be contained in the SDN control plane so that end users see an easy-to-use IoT with significantly improved security, privacy, performance, and energy-efficiency.

A green, deterministic, Industrial-Tactile IoT network consisting of many simple deterministic packet switches under the control of an

SDN control plane has been proposed in prior work.[2,5,6] This network exhibits several attractive properties:

- The SDN control plane can embed millions of mutually exclusive DVNs in layers 2 or 3.
- Unauthorized packets from a cyberattacker can be detected in microseconds in layer 2.
- Congestion, interference, and excessive delays associated with best-effort traffic flows can be removed.
- IoT links can operate at 100 percent of their capacity, saving potentially $36 billion a year in excess capital costs.[2]
- IoT buffer sizes can be reduced by a factor of 1,000 to 1,000,000 times, and IoT transport delays can be reduced to the speed of light.
- IoT energy efficiency can be considerably improved.

A DVN can be organized in two ways: as a virtual IoT subnetwork that is absorbed by the existing IoT and used by the public; or as a virtual intranet that is used exclusively by one entity. Any cloud service provider, such as Netflix, YouTube, or Google, can reserve its own virtual IoT subnetwork to achieve improved security, privacy, performance, and energy efficiency. A virtual IoT can support all existing Internet standards, protocols, applications, and priority classes.

In contrast, a virtual intranet can be created for a single entity that requires exceptional security, privacy, performance, and energy efficiency. A virtual intranet is essentially a private DVN that operates in layer 2. A cyber-physical control system for the smart power grid can reserve its own virtual intranet to manage its resources. Likewise, a government agency such as the US Department of Homeland Security can reserve its own virtual intranet to manage its resources. These virtual intranets are logically disconnected from the BE-IoT and are therefore immune to DoS attacks and cyberattacks.

DVNs can be established for weeks, months, or years and can support data rates ranging from Gbps to Tbps. In this article, the following opportunities are highlighted:

- Deterministic packet switches using silicon-photonics technologies will be feasible in a few years.
- A green Industrial-Tactile IoT using these technologies can pay for itself quickly through reduced capital and energy costs.
- "Lightweight" encryption algorithms can be embedded directly into layer-2 silicon-photonics switches.
- The use of long encryption keys managed by the SDN control plane will become attractive.

Existing encryption schemes such as the Advanced Encryption Standard (AES)[7] and RSA are not well suited to encrypt DVNs with aggregate throughputs of tens to hundreds of Tbps. The computational and energy overheads would be prohibitive. Here, the use of lightweight encryption with long keys embedded in layer-2 DVNs to provide exceptionally strong security and privacy is highlighted.

The proposed green, deterministic Industrial-Tactile IoT can achieve a level of cybersecurity and privacy well beyond that possible with today's BE-IoT. Future smart systems, such as smart cities, smart transportation systems, the smart power grid, and smart healthcare systems, can all reserve their own mutually exclusive DVNs in layer 2, with exceptionally strong security, privacy, performance, and energy efficiency.

Security and Privacy in the BE-IOT

A 2015 ACM SIGCOMM workshop has outlined six basic questions on the performance and security of today's BE-IoT that are difficult or impossible to answer:[8]

- Can packets from source A reach destination B?
- Is traffic from source A and from source B isolated?
- What causes mysterious packet losses?
- Is poor performance of a cloud service caused by the BE-IoT network or the datacenter?
- Why is backbone utilization so poor?
- Is the load balancer distributing the load evenly?

It is extremely difficult to provide cybersecurity, privacy, and trust in today's BE-IoT when such basic questions cannot be answered. These performance problems also incur excess capital and energy costs of tens of billions per year.[2,5,6]

To compound the security problems, the lack of centralized control allows any user to transmit data to any destination at any data rate; thus, it is relatively easy to create a DoS attack that floods a destination with unwanted and useless traffic, causing it to fail.

In 2016, a French webhosting provider, OVH, was targeted with a record-breaking DoS attack exceeding 1 Tbit per second, launched from more than 150,000 compromised smart devices, such as IP-based video cameras. Furthermore, cyberattackers are free to roam today's BE-IoT looking for targets to attack. The proposed approach will remove these threats.

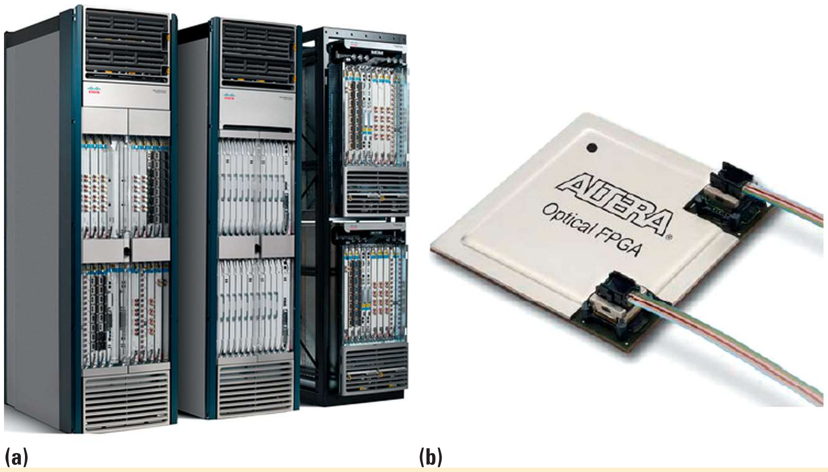

Figure 2. Two designs for terabit-capacity routers. (a) A single cabinet of the Cisco CRS-3 core router has a bandwidth capacity of about 4.5 Tbps and dissipates about 7.8 KW of power (image courtesy of www.cisco.com). (b) This single-chip FPGA with optical IO will soon achieve the same capacity (image courtesy of www.altera.com).

The Advanced Encryption Standard

In 2000, the US government approved the AES for its top-secret communications, with an intended lifespan of several decades.[7] AES is a block cipher, which can encrypt 128-bit blocks of data using small keys with 128, 192, or 256 bits. More recent cryptography mechanisms are described elsewhere.[9] However, in 2015, the US government acknowledged the threat of potential cyberattacks against AES and RSA encryption through the use of quantum computers.[10] To counteract this threat, the US government announced that encryption schemes with longer keys should be used, which would push the threat of quantum computers 20 to 30 years into the future.

FPGAs with Silicon Photonics

Field programmable gate arrays (FPGAs) that are integrated with silicon-photonics optical transceivers should be available within a decade, and these devices will revolutionize network design. Consider Cisco's CRS-3 best-effort Internet router, shown in Figure 2a. In 2016, a single cabinet has a bandwidth capacity of about 4.5 Tbps, weighs 1,600 pounds, and dissipates about 7.8 KW of power.

An integrated FPGA with optical IO is shown in Figure 2b. FPGAs with several Tbits of optical bandwidth will be available soon[5,11] and will transform networks in the 21st century. Deterministic packet switches are ideally suited to FPGAs because they can reduce buffer sizes by a factor of 1,000+ times.[5,6] As determined in prior work, a simple, deterministic packet switch realized on a single FPGA should achieve the same 4.5-Tbps capacity as a Cisco CRS-3 cabinet, while dissipating about 100 W of power.[5] These integrated switches can be used to provide an energy-efficient deterministic layer-2 network that can embed millions of distinct DVNs, as shown in Figure 3a. Lightweight encryption is an active area of research.[12,13] Here, the use of fast, lightweight encryption schemes with longer keys to encrypt and decrypt the nation's IoT data at rates of tens of Tbps within FPGAs is proposed.

A Green Industrial-Tactile Internet of Things

The BE-IoT supports best-effort traffic flows without any performance guarantees. The proposed green deterministic IoT supports deterministic traffic flows (DTFs) and uses simple deterministic packet switches (DPSs). Figure 3a illustrates DTFs in the Internet protocol layer (layer 3) and DTFs in the data link layer (layer 2). Figure 3b illustrates a deterministic IoT network for the US with 28 nodes (cities) and 82 edges. The bold lines represent fiber-optic links between cities. The dotted lines represent DTFs between cities in layer 2. An Internet router in layer 3 views a DTF in layer 2 as a dedicated fiber-optic link with a guaranteed data rate between two remote cities.

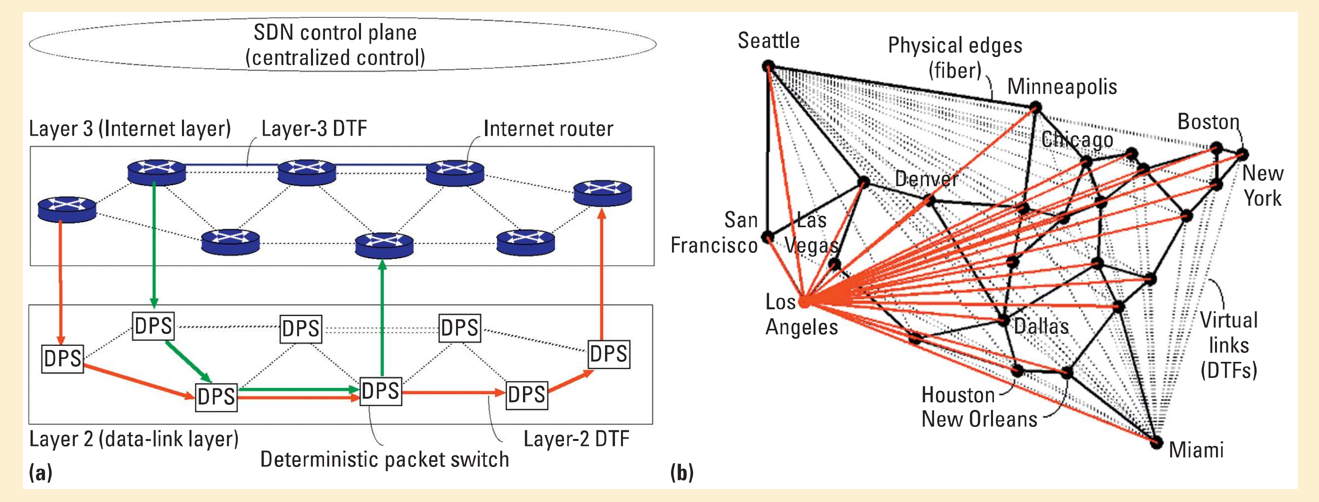

Figure 3. The proposed green deterministic IoT. (a) It supports deterministic traffic flows (DTFs) in layers 2 and 3. (b) This example deterministic IoT spans the US with a deterministic virtual network (DVN) originating in Los Angeles. Congestion-free DTFs from Los Angeles to other cities are shown with bold red lines.

In Figure 3b, three DVNs are embedded in the network. Three cities—Seattle, Miami, and Los Angeles—each have a DTF to every other city in the network. A DVN with 27 DTFs originating in Los Angeles and directed to every other city is shown by the bold red lines.

DTF Properties

The proposed SDN control plane can program millions of DVNs into the deterministic core network in layers 2 or 3, as shown in Figures 3a and 3b. To provide enhanced security, let the DVNs be embedded in layer 2. The following properties hold for the DTFs in layer 2.[5]

Property 1. Every DTF has a deterministic (or guaranteed) data rate to be supported by the network from nodes *s* to *d*. The data rate can be expressed as a guaranteed number of reservations for packet transmissions within a scheduling interval, called the scheduling frame. A scheduling frame can typically have $F = 1{,}024$ time slots.

Property 2. The SDN control plane will route every DTF along a fixed path of layer-2 switches and links in the network. The control plane uses a minimum-cost maximum-flow routing algorithm,[14] which can achieve 100 percent utilization. The SDN control plane can determine two lists: the list of DTFs that arrive at every incoming fiber of a switch and the list of DTFs that depart on every output fiber of a switch.

Property 3. The SDN control plane can compute a deterministic transmission schedule (TX-schedule) for every fiber-optic link leaving a DPS. The TX-schedule will identify the DTF with a transmission reservation for that fiber in every time slot of a periodic scheduling frame. Using the scheduling algorithms from prior work,[6] the schedules can be circularly rotated and still minimize buffer sizes and delays so that the switches do not need to be synchronized.[2]

Property 4. The SDN control plane can compute a deterministic reception schedule (RX-schedule) for every fiber-optic link arriving at a DPS. The RX-schedule will identify the DTF with an arrival reservation for that fiber in every time slot of a periodic scheduling frame.

Property 5. Unauthorized packet transmissions from a cyberattacker that target a virtual intranet DVN can be quickly detected in layer 2. Any packet that arrives (or departs) at a switch in a time slot for which no arrival (or departure) was scheduled will violate the deterministic RX-schedule (or TX-schedule) and must be unauthorized. Such a packet will be immediately detected, and the SDN control plane can be informed for corrective action. The use of deterministic switches creates an inherent *intrusion detection system* for the IoT, in which any intrusions by cyberattackers are quickly detected in hardware. Furthermore, any packet that arrives at a destination in a time slot for which an arrival was scheduled can be decrypted and verified using a lightweight encryption scheme in layer 2. For verification, every valid packet must pass a verification check (see property 6).

Property 6. Let each DTF request a security level, using a logarithmic scale from 0 to 10, from the SDN control plane when it is established. The SDN control plane can then issue an authorization key and lightweight encryption/decryption keys of suitable lengths to each authorized DTF. The authorization key can be a unique, secret, pseudo-random bitstream. Each packet of a DTF can carry the authorization key (or a value derived from this key) for verification. A moderate, high, or very high security level might entail encryption keys with hundreds, thousands, or tens of thousands of bits, respectively. (Ironically, longer keys can improve security and energy efficiency—for example, by reducing unnecessary computations in AES to recompute dependent security keys for each round.)

Security, Reliability, and Cost Considerations

Exceptionally strong end-to-end security, privacy, and trust require three properties:

- The deterministic packet switches cannot be compromised by a cyberattacker.
- The SDN control plane cannot be compromised.
- Communications between switches and control planes cannot be compromised.

The first property can be achieved by designing the switches directly into hardware, which must be immutable. The second property can be achieved by operating multiple copies of the SDN control plane in parallel and by using majority voting logic.[5] It would be virtually impossible for a cyberattacker to compromise multiple parallel SDN control planes simultaneously when each one uses a distinct encryption key. The third property can be achieved using lightweight encryption and verification keys with very long lengths—that is, thousands or tens of thousands of bits. Even quantum computers will have difficulty cracking encryption keys with thousands of bits in the next few decades.[10]

An integrated FPGA with optical IO will reduce energy use and capital costs by 10 to potentially 100 times compared to an existing BE-IoT router,[5] as shown in Figure 2. Furthermore, each DTF between remote cities in layer 2 will bypass potentially five to 10 BE-IoT routers in layer 3, thereby further reducing capital and energy costs by a factor of potentially five to 10 times. Reliability can also be improved by exploiting redundant paths in layer 2, which is far less expensive than exploiting redundant paths in layer 3. From a cost perspective, the use of DVNs in layer 2 will pay for itself quickly by significantly lowering capital and energy costs.

Experimental Results for the US IoT Network

The SDN control plane programmed 320 DTFs into the US network shown in Figure 3b to achieve a link utilization of 93 percent, and the performance was determined. A scheduling frame with $F = 1{,}024$ time slots was used. Each time slot was sufficient to transmit an IPv4 packet over a DTF. Assuming 1,500-byte IPv4 packets and 800-Gbps edges, each time slot has a duration of 15 nanoseconds.

The network performance was determined with a hardware testbed in which 26 simple deterministic packet switches were synthesized on an FPGA. The testbed transmits more than 400 million packets per second. A similar testbed is described elsewhere.[15] The hardware testbed results were identical to the results of a software simulator.

Figure 4a illustrates the end-to-end IoT queueing delays along several DTFs in microseconds. The queueing delays are ≤ 2 microseconds. Consider the DTF between Los Angeles and Miami. The distance between these two cities is about 3,800 km, and the fiber latency exceeds 19 milliseconds. The queueing delay is a few thousand times smaller than the end-to-end fiber delay, consistent with a prior theory.[6]

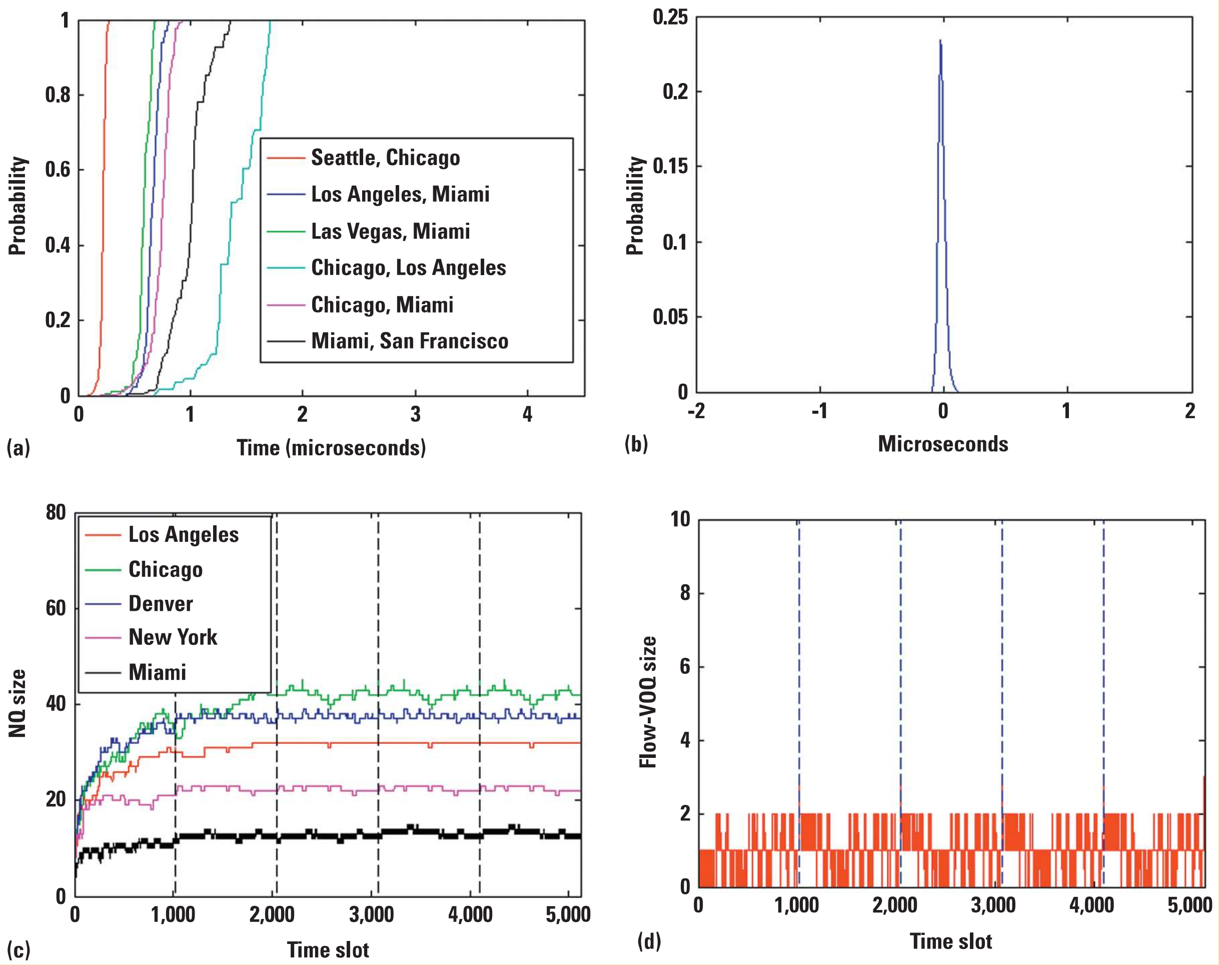

Figure 4. Experimental results. Performance measures included (a) end-to-end queuing delay cumulative distribution function for selected deterministic traffic flows (DTFs); (b) age jitter distribution for all DTFs; (c) packets queued per switch; and (d) packets queued per DTF per switch (typical).

Figure 4b illustrates the jitter of the packets leaving a DTF. These jitters are much smaller than the end-to-end fiber delays in the US network, which are measured in milliseconds.

Figure 4c illustrates the evolution of the number of packets queued in each city versus time, assuming an empty network at time slot 0. The evolution reaches a deterministic pattern that repeats for each scheduling frame. Figure 4c shows that a maximum of about 50 packets are buffered in the Chicago node. The well-known bandwidth-delay product (BDP) buffer-sizing rule provides about 1/4 second of buffering per fiber to provide congestion control in the BE-IoT.[6] Using the BDP rule, the worst-case buffer size in the Chicago node is about 80 million packets. The use of deterministic packet switching has reduced the worst-case buffer sizes from about 80 million down to about 50 packets, a reduction of roughly 1,000,000 times.

Figure 4d illustrates the number of packets in a typical flow queue, which buffers the packets of a single DTF. The packet arrivals and departures to each switch form deterministic processes, with no randomness. As stated in property 5, unauthorized packets from a cyberattacker will violate the deterministic TX or RX schedules in a deterministic packet switch and can be quickly detected.

The future Industrial and Tactile IoT must support the demanding, smart cyber-physical systems of the 21st century, such as smart cities and the smart power grid. Cybersecurity remains an outstanding challenge. This article shows that the combination of a centralized SDN control plane, DVNs, and lightweight encryption in layer 2 can achieve exceptional security, privacy, performance, and energy efficiency in the IoT, in datacenters, and in cloud computing systems. The proposed SDN control plane can embed millions of distinct DVNs into a layer-2 green deterministic host network. The use of deterministic switches creates an inherent intrusion detection system in which the arrival of any unauthorized packets from a cyberattacker, even a single packet, can be detected in microseconds, leading to corrective action by the SDN control plane. As a result, the DVNs are immune to congestion, interference, DoS attacks, and targeted cyberattacks in layer 2. Future smart systems can reserve their own mutually exclusive and interference-free DVNs to achieve significantly improved security, privacy, performance, and energy efficiency well beyond what is possible with today's BE-IoT. IT

References

1. P.C. Evans and M. Annunziata, *Industrial Internet: Pushing the Boundaries of Minds and Machines*, General Electric, Nov. 2012, pp. 1–37.
2. T.H. Szymanski, "Supporting Consumer Services in a Deterministic Industrial Internet Core Network," *IEEE Comm.*, vol. 54, no. 6, 2016, pp. 110–117.
3. G. Fettweis et al., *The Tactile Internet*, ITU-T Technology Watch Report, Aug. 2014, pp. 1–24.
4. M. Maier et al., "Tactile Internet: Vision, Recent Progress, and Open Challenges," *IEEE Comm.*, vol. 54, no. 5, 2016, pp. 138–145.
5. T.H. Szymanski, "Securing the Industrial-Tactile Internet of Things with Deterministic Silicon Photonic Switches," *IEEE Access*, vol. 4, 2016, pp. 8236–8249.
6. T.H. Szymanski, "An Ultra-Low Latency Guaranteed Rate Internet for Cloud Services," *IEEE Trans. Networking*, vol. 24, no. 1, 2016, pp. 123–136.
7. "Announcing the Advanced Encryption Standard (AES)," Federal Information Processing Standards (FIPS) publication 197, 2001, pp. 1–51.
8. G. Varghese and N. Bjorner, "Network Verification," ACM SIGCOMM tutorial, Aug. 2015.
9. E. Barker, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, NIST special publication 800-175B, Mar. 2016, pp. 1–79.
10. A. Nordrum, "Quantum Computer Comes Close to Cracking RSA Encryption," *IEEE Spectrum*, 3 Mar. 2016; bit.ly/1oSxb92.
11. Y.A. Vlasov, "Silicon-CMOS Integrated Nano-Photonics for Computer and Data Communications beyond 100G," *IEEE Comm.*, Feb. 2012, pp. 67–72.
12. J. Borghoff et al., "PRINCE: A Low-Latency Block Cipher for Pervasive Computing Applications," *Proc. Int'l Conf. Theory and Application of Cryptology and Information Security*, 2012, pp. 208–225.
13. A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems*, 2007, pp. 450–466.
14. T.H. Szymanski, "Max-Flow Min-Cost Routing in a Future Internet with Improved QoS Guarantees," *IEEE Trans. Communications*, vol. 61, no. 4, 2013, pp. 1485–1497.
15. M. Rezaee and T.H. Szymanski, "Demonstration of an FPGA Controller for Guaranteed-Rate Optical Packet Switching," *Proc. IFIP/IEEE Int'l Symp. Integrated Network Management* (IM), 2015, pp. 1139–1140.

Ted H. Szymanski *is a professor in the Department of Electrical and Computer Engineering at McMaster University, Canada. His interests include security, energy efficiency, deterministic communications, optical communications, 5G wireless communications, smart cyber-physical systems, and the Industrial and Tactile Internet of Things. Szymanski held the Bell Canada Chair in Data Communications at McMaster University, and led the Optical Architectures project in a 10-year research program in the Networks of Centers of Excellence of Canada. He received a PhD in electrical and computer engineering from the University of Toronto. Contact him at teds@mcmaster.ca.*