dispersive®

SMART CITY RESILIENCE THROUGH SDN

AUTHOR

Chris Swan
Dispersive Networks
Chief Revenue Officer

The Hyperconnected Nature of Urban Life

The Internet of Things (IoT) is everywhere, but there may be no greater convergence of connected devices, cloud applications, and solutions across multiple categories than one can find in Smart City implementations. Given the wide variety of devices attached to the public Internet and private IP networks, managing the geographic distribution of those devices and systems is a massive challenge. Whether in fixed physical infrastructure, mobile smart cars, control systems for public transportation vehicles, or as part of public safety, ensuring these devices can communicate securely across transmission networks has become mission-critical.

The performance of these Smart City networks is also crucial, given the hyper-connected and on-demand public expectations and the nature of urban life going forward.

Challenges to Network Resiliency

As the IoT and related Industrial IoT grow, in large part due to the investment in Smart Cities, resilience is increasingly important. Challenges to network resiliency include responses to large-scale natural disasters that can destroy parts of the network, cyber-attacks by adversaries wishing to take entire cities down, unintentional or intentional actions of insiders, such as network administrators who can hold organizations hostage simply by changing policies using weak network operating systems, and more. The integrity of a Smart City and the data that is generated by sensors, cameras, and other endpoints on its networks are highly vulnerable when legacy network architectures are used without the benefit of Software Defined Networking (SDN). Having to monitor and manage multiple networks, applications, cloud services, and the exchange of data without an SDN strategy and next-generation secure and performant private network in place is unsustainable economically.

Unlock Value, Reduce Risk

This white paper lays out a blueprint for digital city planners, technology architects, networking experts, government agencies, IoT solution providers, and others in the Smart City ecosystem. The creation of ultra-secure, high performance, mission-critical resilient connectivity environments will help unlock the massive value of connected communities while reducing risk.

INTRODUCTION

Increasingly Complex Internet

The public Internet was built for resilience, but since its inception in the last century, the Internet has become an extremely complex series of multi-realm, multi-level networks. The growth of the IoT, which is the most significant driver in digital cities, is dramatically increasing in complexity and expanding the cyberattack threat surface.

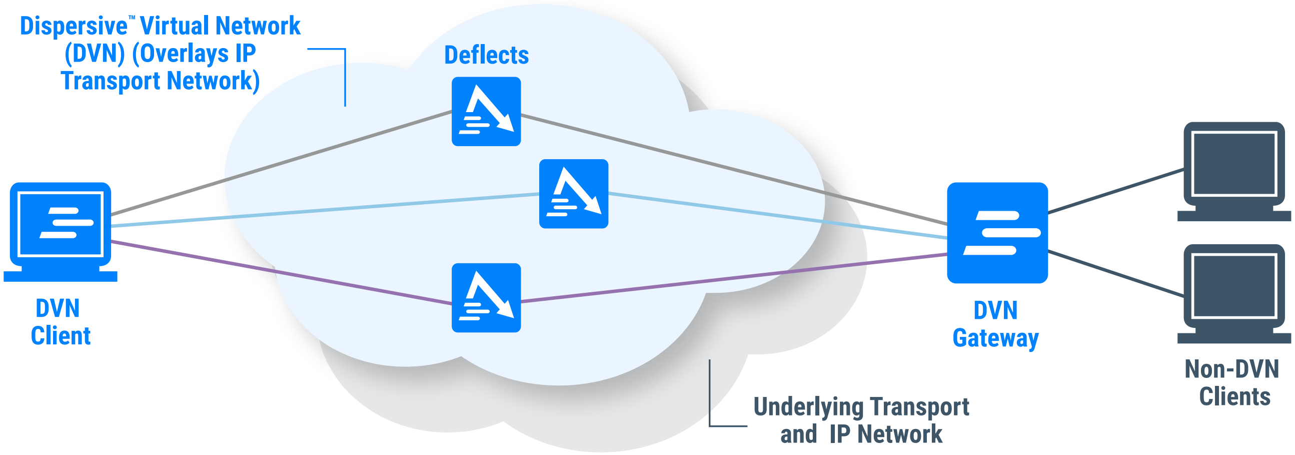
Not only are the number of endpoints increasing due to IoT, but also rising are the number of networks and sub-networks. The increased heterogeneity of protocols, standards, local computing requirements, multi-cloud applications, and the business applications (including connecting the primary energy grid, micro-grids, traffic and safety applications and more) have led to an interdependency among systems that were not designed to communicate with each other. The network must now become part of the solution for normalization and efficiency—and not part of the problem, which it has become today.

Advantage of Software-Defined Networking

Collecting IoT information that dwarfs "big data" projects of the past, analyzing and securing that information, and modeling the adaption of that data for efficient and automated systems is not trivial.

Sub-domains are being managed as "islands" with protected perimeters and independent components for computing (DNS, CDNs, PKI, edge computing for ultra-low latency applications, and more). It is the interdependent applications that create even more pressure for security, including systems sharing information via APIs.

Software-Defined Networking (SDN) provides unprecedented flexibility in that it can dynamically reconfigure IP networks and leverage the scale and natural resilience of the Internet while providing hardened security based on how "events" or "sessions" are treated.


Dispersive™ Virtual Network (DVN) (Overlays IP Transport Network)
Deflects
DVN Client
DVN Gateway
Non-DVN Clients
Underlying Transport and IP Network

Time to Switch to SDN Approaches

"Now Generation" SDN technologies enable more sophisticated network management applications, traffic shaping, Quality of Service (QoS) optimization and applied to smart grids, for example, protect against accidental failures or malicious attacks. SDN has been proven in the electrical energy industry most recently and extended to alternative energy sources, which has forced the overall "ecosystem" to interconnect grids for mission-critical power. While the energy industry has been at the forefront for all the obvious and right reasons, network and application architects across the board are learning that it's time to make a switch to SDN approaches. SDN allows for real-time human communications, machine-to-machine communications, or most importantly, the crossover of messaging between people and things.

With advances in mobile, fixed-edge, and pervasive computing, the exponential growth in Internet applications continues. Innovative IoT services drive smart cities that revolutionize the way we live, commute, conduct business, manage public health, and secure our communities. The fundamental architecture for how all this is connected physically and virtually can significantly enhance and protect against attacks. On the other hand, poor design built on legacy frameworks could bring networks and geographies to a grinding halt, costing billions in damages and resulting in significant loss of life. The next choices we make in designing these networks need careful attention and planning for the future with a solid foundation of proven agile technologies that scale and evolve.

SMART CRITICAL INFRASTRUCTURE

Smart Critical Infrastructure (SCI) enables the deployment of adaptive, reliable, economically feasible, and shared private networks. SCI brings together smart grids with smart homes, buildings, and transportation systems, including electric and increasingly autonomous vehicles, smart homes, buildings, factories, schools, and hospitals.

Done collaboratively and with SDN technology, SCI integrates city government, county/state/federal government, utilities (electricity, gas, water, wind, waste management and more), transportation systems and public safety platforms onto a holistic infrastructure. A connected infrastructure offers day to day management—but also can be leveraged to respond in real-time to natural or manmade disasters.

The integration of physical and cyber systems, as well as human behaviors, can be orchestrated and optimized using SCI.

Current SCADA Solutions

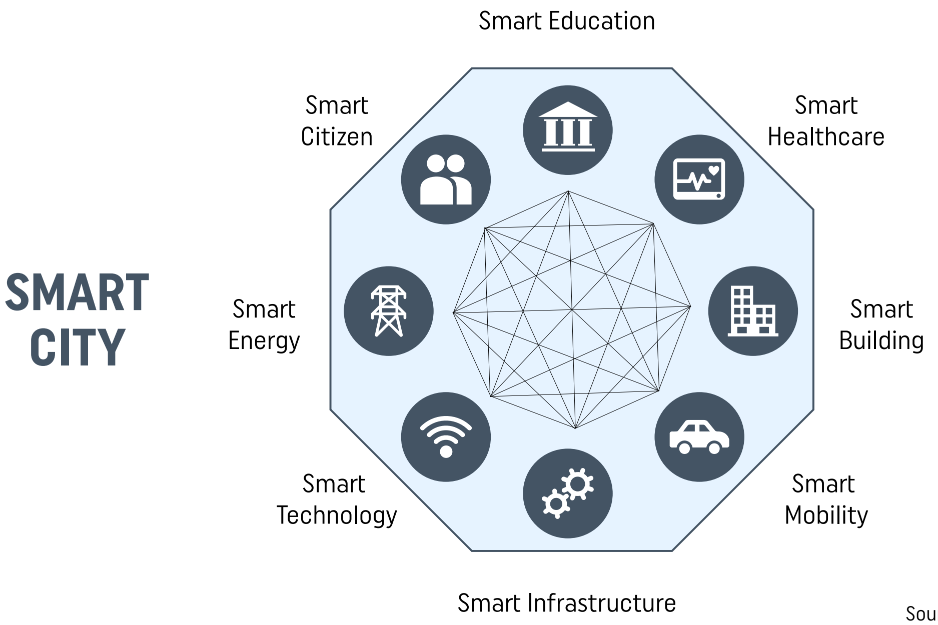
The integration of systems naturally increases the vulnerability and the attack surface at an ecosystem level. However, proven architectures that achieve the successful monitoring and control of critical infrastructures like Supervisory Control and Data Acquisition (SCADA) systems are influencing the way we design smart cities beyond the electrical grid, where SCADA is in use today.

SCADA systems become interconnected with Internet resources and services in Smart Cities (and they are often the foundation of smart city projects). These SCADA systems become attractive targets to external and internal adversaries because they were initially designed to only operate in an isolated environment, completely separate from other private networks and the public Internet.

Today, massive value is created through innovations connecting different networks and systems, including cloud computing applications, which is driving the expansion of the attack surface and exposing new vectors leading to pivot attacks and more.

New SDN Solutions

SCADA network operators are now turning to SDN, and solutions like Dispersive's virtual networking technology, to protect from the execution of malicious commands on control systems and remote devices, protecting against economic disruption and massive threats to human health and safety.



Source: Frost & Sullivan

Three Attacks Which Could Have Been Avoided with SDN Approaches

2003
The Slammer worm infected the computer network at a nuclear power plant, disabling the safety monitoring system for five hours, shutting down the processing system of the plant for six hours, and affected communications on the control networks of other utilities.

2012
A cyberattack occurred against gas pipelines in which bad actors took over the control of valves, switches, and critical processes resulting in an international incident that involved the United States and Canada. In this same year, the number of attacks to America's power, water, and nuclear systems increased by 52%, several of which resulted in successful intrusions.

2015-2016
Russian cyberattacks caused two large-scale blackouts in Ukraine; Russia's continued probing of US critical infrastructure has been proven, and some believe the shut-downs in Ukraine were a "dry run" for attacks to America's grid.

It is essential to understand the history of attacks on critical infrastructure in the power industry, and learn from those how related systems in Smart Cities can be built with the latest networking approaches, securing every device, application, event, session, and transaction, using software innovations that protect data at rest and in motion.

WHAT ARE THE OPPORTUNITIES FOR SDN TO ENHANCE SMART GRID RESILIENCE AND, BY EXTENSION, SMART CITY DEPLOYMENTS?

A key advantage of SDN is its ability to dynamically configure the network, creating and deleting routing paths, preventing failures and attacks, and immediately mitigating attacks if they occur, including isolating them in real-time.

Defending Against Cyber Attacks

SDN is being used today to establish dynamic routes on the control plane, transmitted from a control center to grid devices, which can significantly diminish and even close the window during which an attacker can inject malicious commands.

SDN also protects against malicious rerouting and Denial of Service (DoS) attacks, by detecting activity on the network which can be addressed, constantly "resetting" encryption keys, deflecting packets, and otherwise outwitting attackers. It is proven that SDN significantly raises the bar for attackers, but this varies between SDN technology providers.

With the right run-time configuration, SDN can bring significant benefits to the Smart Cities of the future, when smart city operators and collaborators can securely operate connected systems and defend against cyber warfare.

A RESILIENT VIRTUAL NETWORK LAYER FOR SMART CITY AND SMART CONTROL APPLICATIONS

Critical infrastructures are rapidly evolving to support valuable innovations in digital technologies that make cities safer, cleaner, more affordable, more livable, and more resilient.

With advanced real-time information services, IoT deployments as part of Smart Cities lead to the more efficient management of energy and better resource utilization. The upside is so clear that the proliferation of ubiquitous connectivity to critical infrastructures (electrical grid, utility networks, billing systems, broadband services, and public safety platforms) is driving healthy new economies, new jobs, and the creation of wealth.

Smart Networks

The promise of hyper-connected urban living, however, will not be fully achieved without smart networks in place today and in the future. Dispersive believes these smart networks will be SDN-based.

We are ready to take on and connect the smart systems which are becoming only more complex, dynamic, heterogeneous, and yes—vulnerable to attacks.

We are proud to be working with government agencies, industry consortiums, IoT developers, network service providers, and Smart City visionaries. Together we are designing resilient and smart critical infrastructure architectures that protect communications, controls, and computations that are automating and optimizing everything from lighting to traffic control to gunshot detection and homeland security programs.

It is acknowledged that Smart City Architectural Standards are a work in progress; however, there is evolving guidance available. Please reference the link below for more information: https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFramework_Version_1_0_20180930.pdf

Industrial Internet of Things

The Internet of Things (IoT) today connects not only computers and mobile devices (smartphones and tablets), but sensors, actuators, gateways, and applications, interconnecting smart buildings, homes, and cities, as well as electrical grids, gas, and water networks, transportation systems and more.

Smart Cities move IoT into IIoT, and in that the scope and scale, look like industrial-size deployments and contribute to the positive impact "Industry 4.0" can have on all our lives, not just manufacturing plants. We are building better lives within communities when we take a step back and look at the networks connecting communities across multiple solutions more holistically.