Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Analytics for Threat Detection in Cyber Intelligence Missions

By: Jesse Price

Today's networks are under attack. Whether the target is a commercial network such as Equifax or the networks for the U.S. elections, cyber-attacks are capable of penetrating the most sophisticated security architectures without detection. Operators and government agencies are increasingly seeking out ways to identify threat trends and patterns by using real-time data derived from advanced network monitoring applications. However, these cyber intelligence tools often miss the critical information that can be gathered from the optical transport network. Modern cyber intelligence missions require comprehensive optical network analytics to pair with their current cyber security tools in order to maximize their success rate.

Optical networks complicate standard threat detection applications. Today's long-haul and regional optical networks are rapidly evolving in order to handle the growing bandwidth demands and required high-speed access. As new technology emerges, network service providers are adopting new transport mechanisms including SD-WAN, DWDM, OTN, and 100G+ coherent technologies in order to make the most efficient use of the deployed fiber network. In many cases, despite the growing presence of new signaling methods, legacy communications protocols can also live in the optical network for many years and this presents a unique challenge for the service providers as they are tasked with managing many different protocols within their networks. Carrying different technologies deeply tunneled within the fiber network creates large multi-layered networks that complicate threat detection. It is now common for optical networks to carry anywhere from up to 5 to 10 different signaling technologies on a single fiber, as shown in Figure 1.

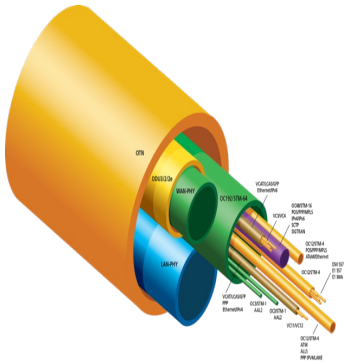

Figure 1: Optical networks support a complex mix of framing and transport technologies.

Not for distribution or reproduction.

Global Optical Transport Networks Are Evolving Rapidly

- ***Global network bandwidth demands doubling every 2-3 years.***
- ***Ethernet standards have evolved from 10GbE to 40GbE to 100GbE and 25/50GbE variants have emerged for datacenter applications.***
- ***Data Center Interconnect (DCI) is driving technology road-map for 200GbE, 400GbE, and 800GbE.***
- ***100G coherent deployments (use of a single DWDM wavelength to deliver 100Gbps) exploded in 2017 while multiple vendors have made recent technology announcements touting the arrival of 400G coherent capable platforms.***
- ***Large carriers have adopted OTN for large-scale optical network transport and transitioned away from SONET/SDH creating a new layer of transport protocols***

Complex optical networks and layers of WAN protocols present network access obstacles for monitoring applications responsible for identifying possible threats and intrusions. Traditionally, cyber intelligence has focused on extracting IP packets off the transport network and performing focused analysis of the IP traffic and the payload carried within. As a result, the transport protocols used in layered optical networks were removed and monitoring applications funneled IP packets to tools responsible for Deep Packet Inspection (DPI) and Distributed Denial of Service (DDoS) detection. Any details regarding how the traffic was transported over the fiber optic network was lost and not accounted for in the traditional cyber threat detection process.

Today, cyber intelligence missions often require monitoring access to long-haul and regional optical networks. Modern surveillance architectures already require a deep understanding of the network infrastructure in order to decode the optical transport mechanism and remove the layers of WAN protocols. But is potentially valuable information being dropped as these network layers are removed? Despite the complexity of the evolving optical transport network, there is valuable metadata that can be extracted from the optical transport signaling protocols that may provide information critical to the success of the cyber intelligence mission.

Optical Network Analytics Offer Unique Threat Detection Details

Cyber intelligence applications are constantly analyzing real-time traffic in order to identify potential network security breaches and looming threats. The large flow of IP traffic is often condensed into a format that is easier to digest and more cost effective to monitor. Standard mechanisms such as IPFIX and Netflow are used by network monitoring tools to summarize IP flows and collect other traffic related information that can be useful for identifying network trends as well as outliers and anomalies. Use of this traffic metadata is one way those responsible for designing threat detection systems can keep traffic analysis costs from becoming unreasonable.

The analysis of metadata from the optical transport network has been proven to be a valuable and effective mechanism for monitoring large flows of traffic. Ignored in most monitoring applications, each layer optical signaling protocol contains information identifying the carrier responsible for transport as well as detailed geographical information that could be used to identify the physical source or destination of the monitored traffic flow. As cyber intelligence solutions attempt to outsmart those responsible for network attacks, an additional layer of optical network analytics opens new opportunities to enhance modern threat detection algorithms.

A wide array of optical transport network parameters are available for use in generating insightful analytics. Network monitoring applications require the ability to perform persistent network discovery in order to extract these parameters in real-time. Examples of optical network parameters that can be extracted in the form of metadata and used to generate optical network analytics could include:

Not for distribution or reproduction.

- Telecom Carrier ID (i.e. AT&T, Tata, Verizon, etc.)
- Network/Fiber ID (i.e. Verizon_seattle_lax_345, etc.)
- Optical Wavelength (i.e. ITU channel 16, etc.)
- Signal Type (i.e. STM-64, 100GbE, OTU4, etc.)
- Geo location and path ID (i.e. Russia to Brazil, etc.)
- Transport Protocol (i.e. GFP, POS, Ethernet, etc.)
- Traffic Volume (changes in traffic patterns may be an indicator of network misuse)

Each of these data points could be analyzed across an entire monitored network or unique network segments. Analysis of these network parameters can be used to characterize the optical network and may be tracked over time to gather historical trends over days, weeks, months, or years. With access to current and historical information, network monitoring applications can identify a baseline for how the network is expected to operate over time but also be capable of detecting abnormal network behavior and potentially providing early warning of a network attack or threat.

Optimal Cyber Intelligence Requires Converged Network Information

Correlating the metadata extracted from the optical transport network with standard IP flow analysis enhances the probabilities of identifying threats by providing a complete picture of the network across all layers: from the physical network to the application data. The increased density of connected devices within the optical network and the fast adoption of software defined networks means topologies and connections can change rapidly – potentially hiding cyber threats. Modern cyber intelligence missions require comprehensive optical network analytics to pair with their current cyber security tools in real-time and in post-mortem analysis to best protect networks from future attacks.

A cyber intelligence solution that combines analysis of IP traffic and its optical transport network forms a threat detection algorithm with access to a much wider and deeper set of information to correlate while searching for network anomalies. Identifying anomalies is the #1 objective of any cyber intelligence mission.

By combining optical network analytics with IP traffic analysis tools, threat detection is capable of identifying:

- Geospatial data using transport network overhead;
- Unauthorized network access due to uncommon provisioning changes;
- Covert communications via presence of new transport channels or new encryption methods; and
- DDoS attack due to spike of targeted traffic from suspect region.

Conclusion:

Networks of all types are seeing increasing attacks as highlighted by several recent high-profile breaches. However, most attacks are not so well publicized. The continued use of optical technologies in the network to support the rapid growth of data, and the push of optical signaling to the edges of the networks underscores the need to be able to monitor at the deepest levels of the optical transport structure in order to help uncover threats and intrusions.

By adding optical network analytics to existing threat detection solutions, network operators can correlate traditional IP traffic flow analysis with the behavior of the optical transport network in order to help determine whether a security threat is emerging and immediate action must be taken to alleviate the threat. The information being tracked via standard optical network analytics fills a void previously de-emphasized by standard cyber intelligence missions.

As new cyber threats are constantly emerging, threat detection solutions must find ways to intelligently correlate all of the data at its disposal even as optical communications networks

Not for distribution or reproduction.

continue to evolve. Information gained via optical network analytics helps to improve the security resilience of today's data networks and can provide greater threat protection.