Understanding Security in Networks with Wireless Connectivity

White Paper

VUBIQ NETWORKS

Making Millimeter Wave Ubiquitous

Executive Summary

In today's digital age, the security of communications systems has become paramount. The increasing reliance on digital transport of voice, video, and data necessitates robust security measures to ensure data integrity, privacy, and protection against cyber-attacks. Encryption remains the cornerstone of securing data networks across government, corporate, and private sectors. This white paper delves into the integration of wireless transport into secured, fiber cable networks, highlighting the efficacy and security of millimeter wave (mmWave) technologies and solutions developed by Vubiq Networks.

Wireless systems using radio frequency (RF) connectivity play a crucial role in modern digital communications. These systems operate across various applications, each with unique performance parameters. Understanding the physical layer of wireless systems, including the transmitter, receiver, and antenna, is essential for grasping how secured digital traffic is maintained across wireless transmission paths.

Antenna radiation patterns are pivotal in wireless security. Omnidirectional antennas used in cellular and Wi-Fi networks offer broad coverage, making them easily accessible and, consequently, more susceptible to eavesdropping. In contrast, highly directional antennas used in mmWave communications form narrow "pencil beams," significantly reducing the risk of interception.

Comparing mmWave links with fiber optic cabling, the white paper highlights that intercepting a mmWave RF beam is far more challenging than tapping a fiber cable. Optical fiber cables are prone to undetectable tapping using off-the-shelf couplers, while mmWave links offer a low probability of intercept, making them one of the most secure wireless communication methods available.

Encryption is the bedrock of network security, ensuring end-to-end protection of data across the network. This white paper discusses various encryption techniques, from IPsec at Layer 3 to MACsec at Layer 2 and optical encryption at Layer 1, emphasizing that end-to-end encryption minimizes the network's attack surface.

Vubiq Networks' HaulPass Fiber product exemplifies this approach by transparently transporting encrypted payload data, maintaining security without introducing redundant hardware or additional latency. As the industry's first software-defined networking mmWave radio, HaulPass Fiber is truly "wireless fiber." Simply plug the API-driven radio into an existing fiber optic network and instantly extend the fiber wirelessly.

In summary, this white paper asserts that network security is defined not by the medium—fiber, copper, or wireless—but by the encryption methods used to protect data. The Vubiq Networks HaulPass Fiber stands out as a superior solution for high-speed wireless transport, offering a secure, efficient, and future-proof method to extend fiber networks.

Table of Contents

1 Introduction

Global internet and communications systems are dealing with ever more demanding security requirements. Voice, video, and data are transported digitally through private and public networks. Security has become so important that standards have been introduced over the past years to address concerns about data integrity, privacy, and protection against cyber-attacks. Government, corporate, and private organizations all make use of data networks; the proven security solution has been and continues through the use of *encryption*.

Designing encryption into a network that also contains wireless transport does not affect the strength or resilience of the encrypted traffic. However, there have been concerns raised about wireless, mainly due to the perception that wireless in general is more susceptible to eavesdropping or being intercepted compared with other media. The purpose of this whitepaper is to provide a good understanding of how wireless systems and wireless transport works, and how wireless transport can combine seamlessly with secured networks. Specifically, we will show how the latest millimeter wave technologies from Vubiq Networks provide robust, end-to-end protection when integrated into well-designed, highly secured networks.

2 Wireless – A Short Tour

In order to understand how network security works in wireless applications, it is important to see how wireless systems themselves operate. The term "wireless" is currently and generally used to describe the use of radio frequency (RF) connectivity over a wide range of applications. Table 1 below summarizes some examples of wireless systems. Each application has its own unique set of performance parameters. Note the listed cases are not exhaustive for the wireless industry; they were selected to represent relevant mainstream examples of present-day digital communications systems.

Table 1. Example Wireless Systems

System	NFC	Bluetooth	Wi-Fi	Cellular	Microwave	Millimeter Wave
Frequency	13.56 MHz	2.4 GHz	2.4, 5, 6 GHz	700 MHz - 2 GHz; 28 GHz	1 GHz - 30 GHz	30 GHz - 90 GHz
Range	<20cm	<50m	~100m	250m - 10km	1km - 50km	500m - 10km
Type	Proximity	WPAN	LAN	WAN	PTP/PTMP	PTP/PTMP
Antenna Pattern	EMB Small	EMB Small	EMB Small/EXT	Omni/Sector	Narrow	Very Narrow

Definitions

NFC	Near Field Communications	EMB	Embedded Antenna
PTP	Point to Point	EXT	External Antenna
PTMP	Point to Multipoint	Omni	Omnidirectional Antenna
WPAN	Wireless Personal Area Network	Sector	Directional Sector Antenna
LAN	Local Area Network	Narrow	Directional Antenna
WAN	Wide Area Network	Very Narrow	Highly Directional Antenna

In the context of wireless security, an understanding of how different wireless applications work is fundamental to knowing how secured digital traffic can be maintained across the transmission path. In networking jargon, there is always a *physical* (or "PHY") layer that represents the physical medium used for transmission[1]. For wireless, the PHY layer is composed of the transmitter and receiver at the endpoints, the antennas used, and interestingly the *empty space* in between. The shape of the space can be thought of as the coverage area, ranging from very close proximity measured in centimeters (cm), such as tapping a payment card with NFC, up through longer distance systems measured in kilometers (km).

The antennas for a cellular base station or a Wi-Fi router are purposely designed to provide coverage nearly equal in all directions, since the location of the users can be anywhere in the coverage area. Think of the base station or router as being located at the center of a circle, with the intention of having randomly located users within that circle able to access the associated wireless service. The only difference in coverage area for these two examples is the size of the circle.

Cellular and Wi-Fi systems span the radio spectrum frequencies from about 700 MHz up through 6 GHz, known as the UHF and the lower microwave RF bands. Recent 5G cellular technologies have also extended into the upper microwave bands up through 30 GHz.[2] These frequency ranges are naturally conducive to broad coverage wireless networks due to the ways UHF and microwave antennas can be designed for omnidirectional, broad sector, and beam-steering. How the RF energy is spread into the coverage area is graphically represented by an *antenna radiation pattern*.

3 Antenna Radiation Patterns

Figure 3 shows some examples of antennas used for cellular base stations, both macrocell and microcell, and small Wi-Fi router antennas. Note that a typical macrocell antenna is actually sectorized, so that it covers a full 360°, but in separate directional sectors. The newer 5G cellular systems are also using methods to steer a more focused beam towards the user, but the aggregate steering range must still cover all directions around the cell site to reach all the users.

Figure 3. Omnidirectional Antennas: Macrocell, Microcell, and Wi-Fi Router

Figure 4 shows how antenna radiation patterns are represented graphically. Notice that the coverage for this example antenna is basically omnidirectional, with the pattern showing fairly equal coverage in all directions when viewing the antenna from the top, looking down like in a plan view.

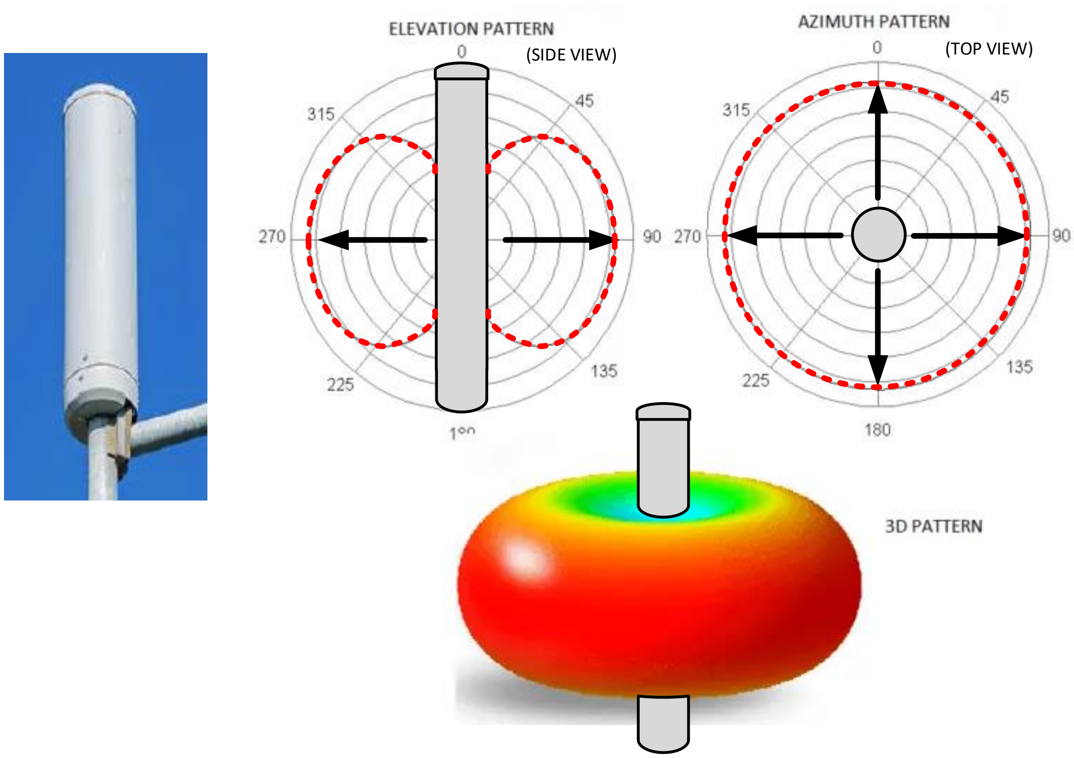

Figure 4. Example Omnidirectional Antenna Radiation Pattern

Example coverage areas for these antenna types are shown in Figure 5. All are basically omnidirectional, but with different size areas, from tens of km for a cellular macrocell down to tens of meters for Wi-Fi in the home.

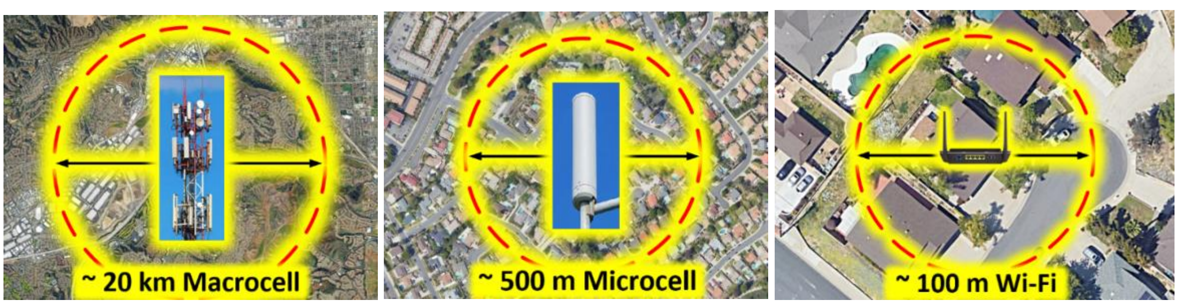

Figure 5. Typical Omnidirectional Coverage Areas for Macrocell, Microcell, and Wi-Fi Router

Omnidirectional or broad radiation pattern antennas makes the services they support very easy to access. As an illustration, there are available apps for mobile phones that can show the nearby Wi-Fi access points and can display signal strength, network addresses, and which RF bands and Wi-Fi channels are being used within the vicinity of the user. An example of a Wi-Fi monitoring application[3] is shown in Figure 6.

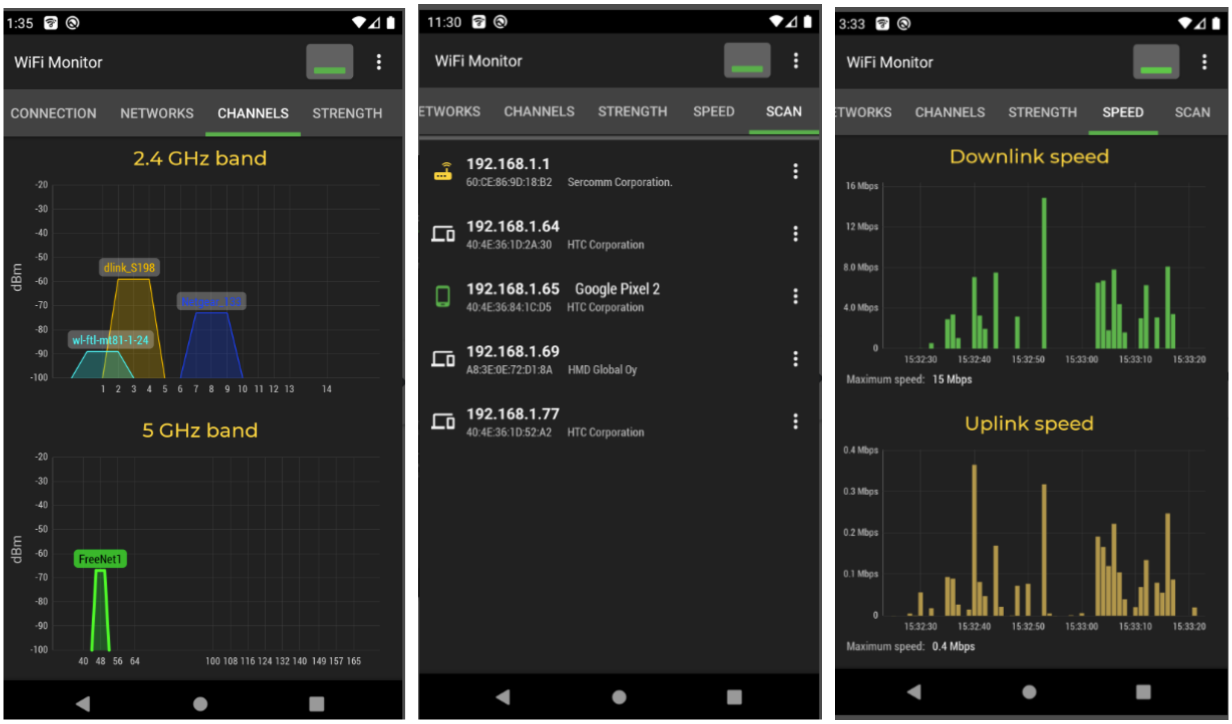

Figure 6. A Wi-Fi Monitoring Application Showing Various Wi-Fi Network Parameters

The point here is that the common experience for users of cellular and Wi-Fi networks is that the users can be just about anywhere, and the coverage is ubiquitous and pretty much taken for granted. The common experience of “wireless” is that it is omnipresent and easy to access, and from a security perspective, easy to eavesdrop or intercept. However, there are many other wireless systems that typical users are most likely not aware of, especially the wireless links behind the scenes that support cellular infrastructure to augment wide area fiber networks. There are many locations where fiber is not available, and high-speed wireless point-to-point links fill in the gaps. This is known as *wireless backhaul*, and in order to support the never-ending demand for bandwidth, higher and higher frequencies are being used that can support higher and higher bandwidths. Moving from microwave up through and past the 30 GHz region is known as millimeter wave (mmWave), which spans frequencies up through 90 GHz.

4 Millimeter Wave Wireless

For establishing private, point-to-point wireless connectivity, higher-frequency microwave and mmWave bands are used. The higher the RF frequency, the higher the available bandwidth, and the easier it is to control using very tight or narrow antenna beam patterns. Two widely used bands in the mmWave frequency range are V-band, at 57 to 71 GHz, and E-band, spanning 71 to 86 GHz. In most regions the E-band frequencies are allocated into two sub-bands, 71-76 GHz, paired with 81-86 GHz, designed for enabling full duplex operation, which is the best way to emulate fiber speed and latency.

Think of a mmWave directional antenna as forming a narrow “pencil beam” radiation pattern. These narrow beams are necessary to enable the required link distances by focusing the RF power into very small, directional patterns, which also insures very little or no interference between different links if they are located in the same general area. Figure 7 illustrates some of the directional antenna types used for mmWave communications.

Figure 7. Example of Directional, Narrow Beam mmWave Antennas[4]

These highly directional, very narrow antennas have a radiation pattern that is illustrated by the model patterns shown in Figure 8. The antenna modelled in Figure 8 is a parabolic dish, and is used often with mmWave point-to-point links forming patterns that produce beamwidths of typically less than one degree in width.

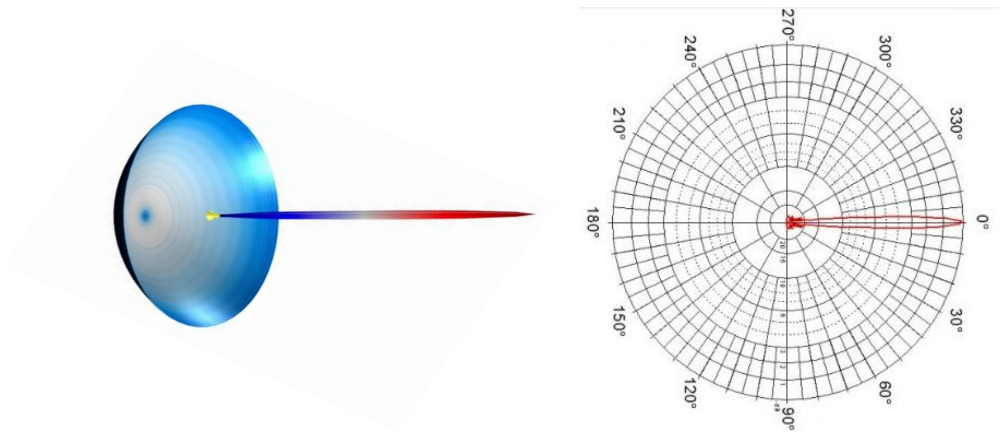

Figure 8. Narrow Beam Parabolic Antenna Patterns for mmWave

The fact that the mmWave antenna pattern is so narrow makes it extremely difficult to access or intercept as compared with the omnidirectional patterns used for cellular and Wi-Fi. As a real-world example, Vubiq Networks installed an E-band point-to-point test link in the Dana Point area of southern California that operated from 2020 through 2023. The link distance was 3.7 km and hosted a 10 Gbps full duplex connection during the test period. The antennas used were 30 cm parabola dish type with a beamwidth of 0.7 degrees. The illustration in Figure 9 shows the endpoints of the link and the narrow-beam path between plotted on a satellite map of the area.

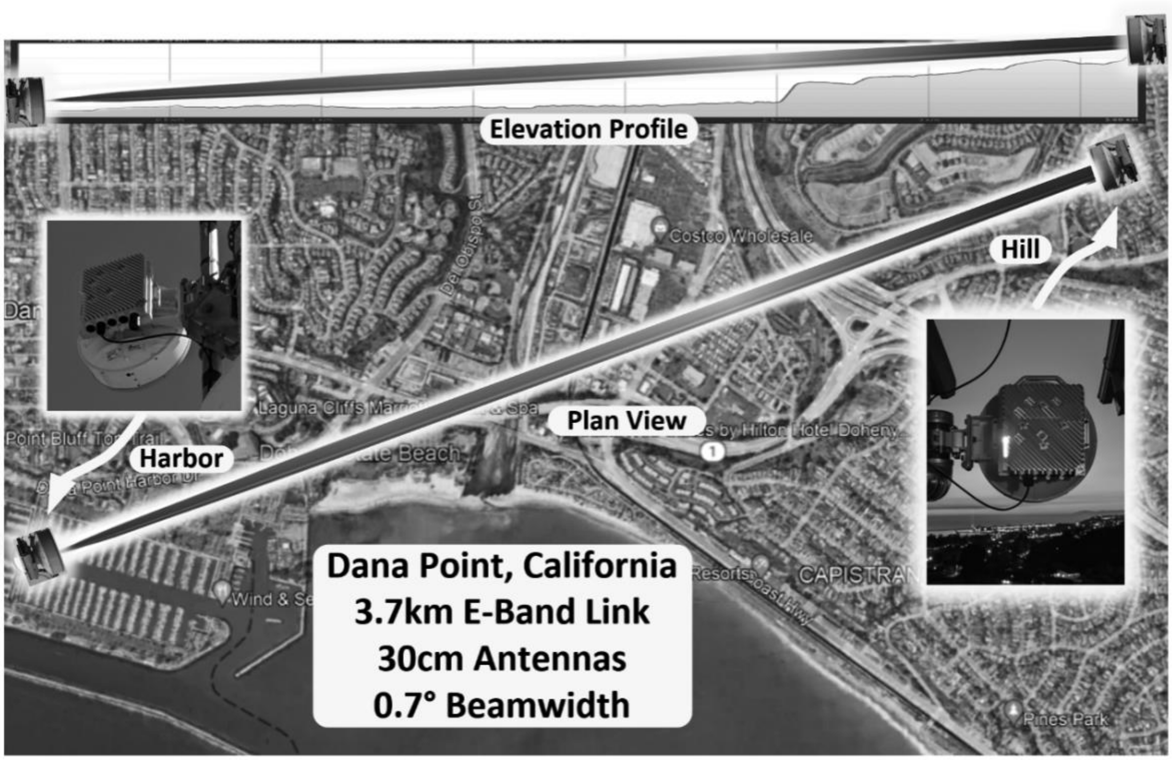

Figure 9. Dana Point E-Band Link, 3.7 km, 10 Gbps Full Duplex with Plan and Elevation Views

5 Characteristics of mmWave Links Versus Fiber Optic Cabling

The RF PHY layer of a mmWave link has such a low probability of intercept (ability to effectively eavesdrop) that even the military uses both 60 GHz[5] and 80 GHz systems for stealth communications. The fact that mmWave is so difficult to intercept makes it one of the most secure methods for wireless communications.

Of note, it is actually easier to intercept and tap a fiber cable than to intercept a mmWave RF beam. Optical fiber cable tapping has been known about for years[6]. Figure 10 is a photo of an off-the-shelf fiber coupler that can be used to tap into a fiber cable without detection[7]. The coupler detects a small amount of light leaking through a bend the fiber cable cladding and is passed on to another network connection allowing an easy method for a hacker to eavesdrop.

There are even online instructions on how to use such a coupler[8]. Figure 11 shows a diagram for tapping into a fiber cable from these instructions. In thinking about fiber, cabling and wireless, any physical fiber optic cable is much easier to access than the RF beam of a mmWave link.

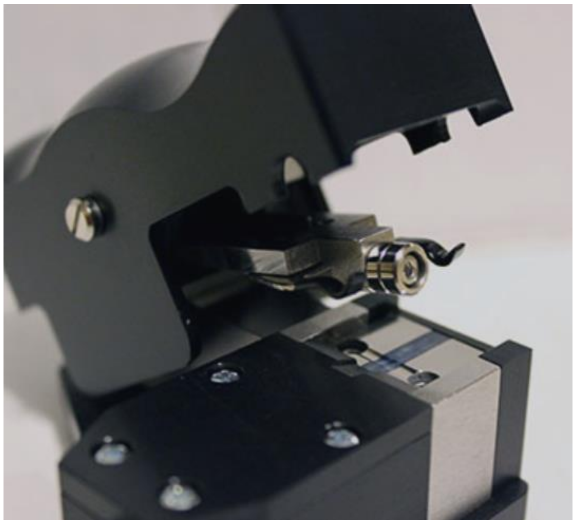

Figure 10. Fiber Optic Coupler for Tapping Without Detection

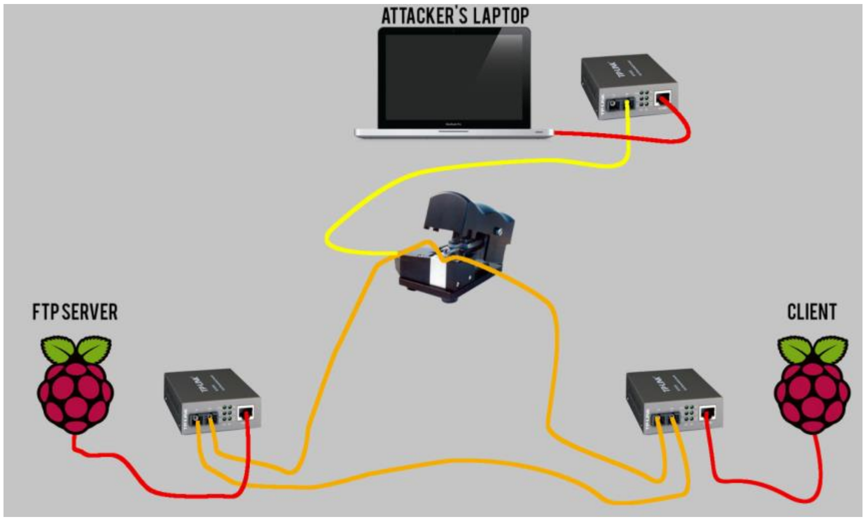

Figure 11. From the Online Instructions on How to Tap a Fiber Optic Cable

So, as it turns out, a network that uses optical fiber or copper for cabled connections is exposed to tapping anywhere along the cable route, near the network routers and switches, and at numerous locations within the same building. Adding a mmWave RF link to that network does not increase the risk of hacking. In fact, an argument can be made that the portion of the network that runs over a mmWave link is less susceptible to compromise than the portion that runs over a physical cable. *The best way to prevent a security breach is to use end-to-end encryption.* This means that any portion of the network can be exposed without concern for compromise. All traffic is encrypted, and therefore safe.

6 Encryption

The type of encryption used will depend on the level of protection desired and the impact on network cost. In the U.S., all non-federal organizations can now make use of publications addressing methods of providing robust and secure network design. As an example, dealing with many different aspects of security, is the NIST SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations[9]. The SP 800 document specifically references FIPS-140-3[10] (now superseding FIPS-140-2[11]) for cryptographic protection. FIPS-140 then references AES Key Generation Requirements[12], with parsed keys either at 128-bit or 256-bit lengths.

Encryption can be implemented at any of the OSI network layers. End-to-end encryption, by definition, assures security across the entire network. Encrypting only a section of the network leaves the unencrypted portions vulnerable. Figure 12 shows several different approaches to implement network encryption at the various network layers. Note that IPsec and Transport Layer encryption, including SSL, protects the payload data (shown in green). IPsec has been in use many years, and there are many variants implemented from countless vendors. It authenticates and encrypts packets using cryptographic keys. IPsec follows the IETF recommendations (for example see RFC6071[13]).

Figure 12. OSI Network Layers Shown with Various Encryption Schemes

A later standard for encryption was introduced by the IEEE[14], called MACsec, and is implemented at Layer 2. Note in Figure 12 that MACsec protects not only the payload frames, but also the MAC addresses. It is a newer security protocol, and is simpler to implement than IPsec, but there are not as many vendors with MACsec capabilities. However, MACsec overhead is lower than IPsec, and is being adopted by the larger cloud service providers such as Microsoft Azure and Amazon AWS. MACsec is port-based, and is built into many of the Ethernet physical port devices (Ethernet PHY) directly in the silicon, which also does not require special software for implementation.

Layer 1 optical encryption, or L1 OE, is the most robust of all techniques, since all Ethernet frames, including the preamble and inter frame gap, are encrypted. It is also the most expensive since the routers and switches in an L1 OE network must be equipped with specific hardware that enables the optical transport to encrypt every bit of data that is sent and received.

It should also be noted that as the encryption technique moves down the OSI layers, the latency introduced decreases. Examples: IPsec, at Layer 3, introduces delays measured in milliseconds (ms); MACsec, at Layer 2, will introduce less latency, in the microseconds (µs); and at Layer 1, optical encryption will add very little latency measured in nanoseconds (ns). Latency in modern networks has become an important consideration due to more stringent application requirements and is now a key parameter, and in many cases has moved to an equivalent status to throughput.[15]

What is important to understand about network security and encryption, is that it must be implemented *end-to-end* in order to protect all facets and locations in the network. For example, if only a specific portion of a network is protected, the other unprotected portions allow what is known as an "attack surface[16]" of unprotected vulnerability. The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect. The goal obviously for a completely secure network is a zero-percent attack surface, which is the goal of end-to-end encryption.

7 Vubiq Networks HaulPass Fiber: Encryption Transparent

The Vubiq Networks HaulPass Fiber, a millimeter wave wireless point-to-point link product, transports all security and encryption network protocols in the same manner as a fiber connection. Nothing is added or deleted: All user payload data is transparently sent between the link terminals. As the industry's first software-defined networking mmWave radio, HaulPass Fiber is truly "wireless fiber." Simply plug the API-driven radio into an existing fiber optic network and instantly extend the fiber wirelessly.

The HaulPass Fiber block diagram is shown in Figure 13.

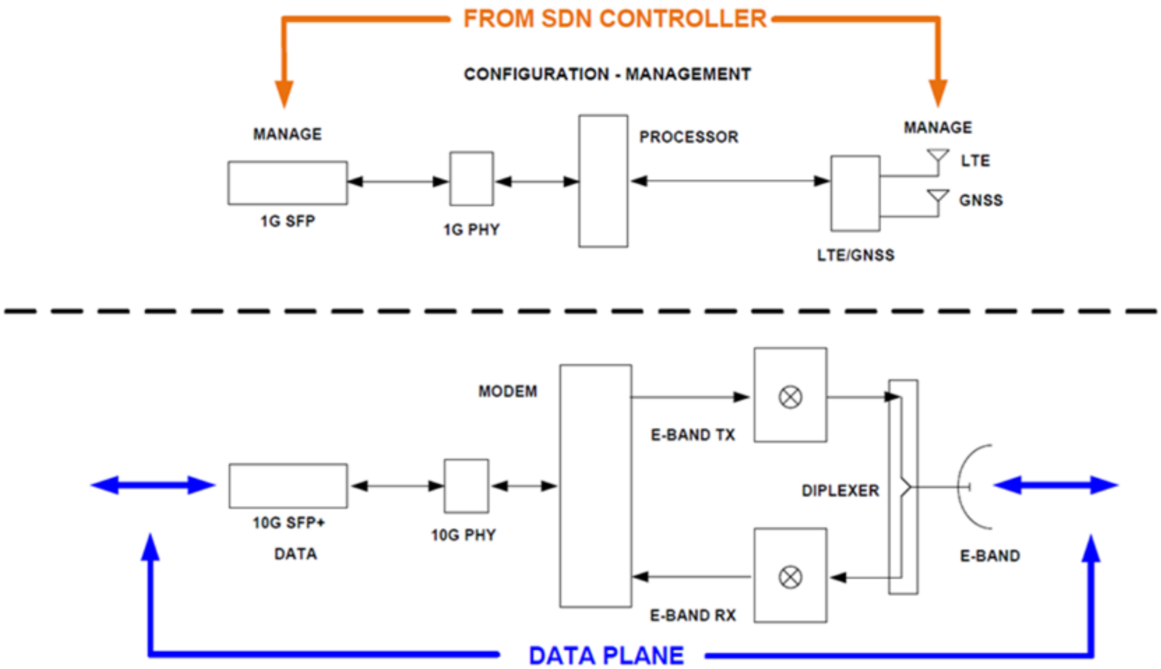

Figure 13. HaulPass Fiber Block Diagram

By design, the HaulPass Fiber physically separates the data plane from the management plane. The payload is never touched, in a hands-off manner, so that any form of encryption, even with anticipated future encryption protocol enhancements, is accommodated. What this means to the user is a future-proof product. Also, by design there are no switches or routers in the link terminals – the payload connections are directly connected to the full duplex RF modem path. The results from this architecture are lower latency, lower power, easier management, and full transparency.

Figure 14 is a diagram of how an encrypted payload is transported through the HaulPass Fiber wireless link. Any form of network encryption, from optical Layer 1, up through the Transport Layers, will be sent unincumbered through the link.

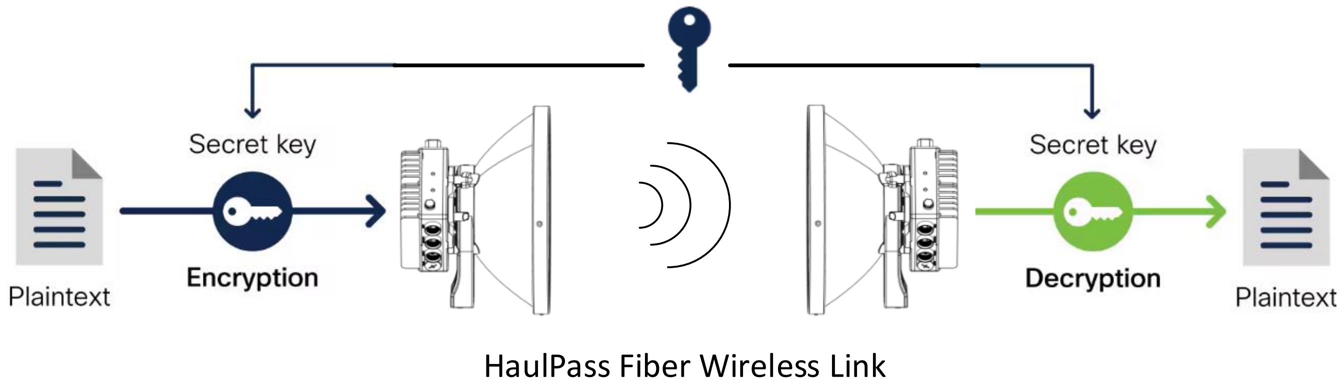

Figure 14. HaulPass Fiber Link Transporting Encrypted Data

The most efficient implementation of network security in a user network is readily accomplished in the network routers and switches that can host the latest versions of encryption standards. If an encryption standard upgrade takes place, the HaulPass fiber agnostically transports the newly encrypted payload. Adding redundant encryption at the radio level would incur additional hardware with the associated increases in power, heat, and most importantly, a large increase in operating latency.

8 Summary

In summary, it is important that network security for both wired and wireless must be viewed as an integrated end-to-end system. Key takeaways from this white paper include:

- Wireless systems vary markedly in characteristics and coverage areas
- The antennas in a wireless system define how the RF energy is distributed
- Omnidirectional wireless like cellular and Wi-Fi provide broad area coverage
- mmWave point-to-point wireless links provide targeted, very narrow pencil beams
- mmWave point-to-point wireless links are inherently secure due to the narrow beams
- Optical fiber cable is inherently not secure due to the ease of tapping the fiber
- The solution for network security, whether cabled or wireless, is full end-to-end encryption
- The Vubiq Networks HaulPass Fiber millimeter wave product transparently passes encrypted payload data.
- By design, the HaulPass Fiber directly connects the network fiber to the radio offering lower latency, lower cost, lower power, all hosted in the smallest physical form factor in the industry.

9 Conclusion

The crux of this white paper: Network security is not defined by the medium used, whether fiber, copper or wireless. Network security is defined by the method used to protect the payload data itself, using encryption.

The Vubiq Networks HaulPass Fiber is, in essence, just like a run of passive fiber – all payload data, including all encrypted payload data, is transparently sent through the link. By keeping the mmWave link design simple, payload transport is enabled without the introduction of redundant network switching elements or unnecessary added latency. Efficiency, future proof, and easy network integration make the HaulPass Fiber the best choice for high-speed wireless transport.

Footnotes:

1. https://en.wikipedia.org/wiki/Physical_layer
2. https://en.wikipedia.org/wiki/Ultra_high_frequency; https://en.wikipedia.org/wiki/Super_high_frequency
3. https://signalmonitoring.com/en/wifi-monitoring-pro
4. Courtesy Prose Technologies https://www.prosetechnologies.com/productDetail.html?rootId=661&id=335&childId=335
5. https://www.microwavejournal.com/articles/42167-mmwave-tactical-communications-platform
6. https://en.wikipedia.org/wiki/Fiber_tapping; https://www.ciena.com/insights/videos/In-the-Lab-Hacking-an-Optical-Fiber-Line-in-Minutes.html
7. https://www.maytelecom.com.cn/optical-clip-on-coupler/
8. https://joshruppe.com/fiber-optic-tapping-tapping-setup/
9. https://csrc.nist.gov/pubs/sp/800/171/r3/final (May 2024)
10. https://csrc.nist.gov/pubs/fips/140-3/final
11. https://csrc.nist.gov/pubs/fips/140-2/upd2/final
12. https://standards.ieee.org/ieee/1619/4205/ (IEEE Standard for Cryptographic Protection…)
13. https://datatracker.ietf.org/doc/html/rfc6071; https://en.wikipedia.org/wiki/IPsec
14. https://1.ieee802.org/security/802-1ae/
15. Latency Tail Wags the Network Dog www.nextplatform.com/2018/03/27/in-modern-datacenters-the-latency-tail-wags-the-network-dog/
16. https://www.fortinet.com/blog/industry-trends/smart-buildings-new-attack-surface

Making Millimeter Wave Ubiquitous

Vubiq Networks, Inc.
9231 Irvine Blvd, Irvine, CA 92618 USA
www.vubiqnetworks.com