All Signs Lead to LiFi

Alistair Banham, Sarah Scace, Ron Schaeffer and Mostafa Afgani

pureLiFi, 51 Timberbush, Leith, Edinburgh, EH6 6QH, Scotland, U.K.

Keywords: LiFi, Light Communications, Optical Wireless Communications.

Abstract: All signs lead to LiFi. Global communications requirements for greater bandwidth, reliable communications, ultra-high speeds and unprecedented security can only be delivered by introducing LiFi to the communications mix. Using light instead of radio waves to send and receive data, LiFi's security, safety and bandwidth advantages make it the right solution at the right time.

1 INTRODUCTION

LiFi is approaching a watershed moment in communications. After an accelerated period of maturation, embeddable LiFi components are now available, and advancements in speed, cost reduction and standardisation mean that LiFi is now ready for those driving next generation consumer technologies that will fill our homes, streets, offices, and public spaces in the next few years.

pureLiFi and the United States Army rolled out the world's first largescale deployment of LiFi in 2021, and the same benefits of high capacity, low latency and security that make LiFi attractive for defence users carry over directly to mainstream use cases.

Data hungry technologies such as AI, AR and IoT connecting everything are in demand and on the rise. The radio frequency (RF) spectrum is suffering from increased congestion due to the increase in connected devices, despite new spectrum being opened up. Schools in several European countries including France and Germany are banning the use of WiFi in schools. Cyber security is no longer just a concern for National Security; it's now a concern for personal security. All industries must now look beyond radio frequencies and LiFi is ready.

2 LiFi CAN DELIVER THE NEXT GENERATION OF USER EXPERIENCES

The McKinsey Global Institute (Grijpink, et al., 2020) estimates that only about 70% of the global demand for digital connections leading up to 2030 will be satisfied by existing radio frequency (RF) and related technologies, even with advancements such as 5G and WiFi 6. That leaves a market worth $600 billion for emerging—or "frontier" technologies like LiFi. McKinsey says, *"With its improved speed, efficiency, latency and coverage, frontier connectivity can produce the remainder by taking many existing use cases to the next level—and paving the way for entirely new ones that we cannot foresee today."* (Grijpink, et al., 2020)

Unable to meet the future demand for wireless communications, it's clear that even cutting-edge RF technologies face the fundamental challenge of limited radio spectrum availability, often called the "spectrum crunch". (Scrogill, 2017) That's where light-based wireless technologies like LiFi step in to bridge the gap, offering 2,600x greater capacity than the radio spectrum.

Changing behaviours and emerging use cases will ensure that exploding demand for digital connections is not just a short-term blip on an otherwise steady upward curve and that RF technologies will struggle to cope. As the International Society for Optics and Photonics points out (Venugopal, 2021), optical wireless communication such as LiFi is set to play an important part in 6th generation (6G) as what may now seem like use cases straight out of science fiction become commonplace. The challenge of conveying emotion in the metaverse aptly demonstrates the hurdles that RF may struggle to surmount.

"Consider that a realistic 3D hologram of a human face requires 19.1 gigapixels. Updating these points in real time to match gestures and expressions will need a download rate of 1 terabit per second!

Similarly, truly immersive augmented reality and virtual reality require high data rates."

Only LiFi—not RF—has a realistic chance of reaching such high data rates. In fact, as part of an international program called Terabit Bidirectional Multi-user Optical Wireless System (TOWS) for 6G LiFi, they hope to propel LiFi to an "eye-watering" terabit per second as soon as 2024. (Pool, 2021)

The world is on track to need the speed and capacity that only LiFi can deliver. Coupled with fast-growing demand by those who are already connected, further accelerated by the pandemic, McKinsey estimates (Grijpink, et al., 2020) that an additional 2 billion users may come online by 2030.

2.1 LiFi Makes RF Better

One of the biggest influencers on user experience is bandwidth. It is a common scenario for users in a typical household to experience poor quality connections due to multi-user effect. For example, video conferencing calls can be throttled due to UHD video streaming in another room. With the introduction of new high bandwidth technologies such as VR in the home, this scenario will only get worse.

Current RF technologies are struggling to service our increased demand for bandwidth. Over 2020 on average users experienced an increase in video buffering by 20%, an increase in video start failures of 19% (Conviva) and a 100% increase in bad link minutes (WiFi now global), all adding up to a significant degradation in our collective user experience online. Technologies such as WiFi-6 are being introduced to combat these challenges, however with limited spectrum the same challenges of congested spectrum will imminently arise.

In 2018 pureLiFi demonstrated in a Scottish school (Schofield, 2018) how LiFi can make Wi-Fi networks more reliable and improve the user experience. A LiFi network was deployed in a classroom that regularly streamed high bandwidth educational videos. By offloading bandwidth-heavy content to the LiFi network, the neighbouring classrooms benefited from more reliable WiFi connections and therefore better user experiences.

LiFi in our homes will have the same benefits. A simple way to introduce the benefits of LiFi to the home is to create LiFi "bubbles" that are positioned in locations of high bandwidth traffic, such as above the TV or in home offices. LiFi could enable both mobile access in these areas and also point to point connectivity for streaming videos, connecting accessories such as sound bars and gaming.

Figure 1: LiFi in use in a classroom at Kyle Academy in Ayrshire Scotland.

By using LiFi-enabled devices and lights in high bandwidth areas of the home it's possible to stream higher resolution videos and games while also enabling more reliable WiFi network for everything else we need to do online.

2.2 Enabling the Future of Immersive Digital Realities

The use of AR and VR is on the rise not only for consumer gaming but in manufacturing environments. Lockheed Martin reports that the use of AR and VR allows engineers to work 30 percent faster and with an accuracy of up to 96 percent. (Popular Mechanics, 2015) However, deploying new mobile technology that requires high bandwidth, low latency connections is a challenge as manufacturing environments are notoriously highly congested RF environments. Security is also a growing concern. Providing LiFi connectivity at the point of need in manufacturing environments can provide highly reliable, low latency connections that are inherently secure.

In the consumer marketplace, Facebook announced their new name Meta in October 2021 reinforcing their strategy to deliver a truly immersive metaverse to its users. As they explore the immersive experience of the metaverse, users will both generate and consume a huge volume of data -- at the edge and at the data centre. Immersion demands an untethered experience, and therefore that data must be delivered wirelessly. Existing RF systems simply will not cope due to their reliance on congested spectrum.

The metaverse will also demand ultra low, and most importantly, consistent latency and jitter. The

metaverse will be real time, so connectivity needs to be real time, too. In testing. LiFi consistently delivers much better performance on these key factors than does WiFi. Figure 2 Illustrates tests performed by pureLiFi comparing pureLiFi's latest LiFi enabled phones for WiFi vs LiFi performance. As illustrated in real world scenarios LiFi performance is higher speed, more consistent and reliable. The tests were performed with identical smartphones operating on the same single channel 802.11ac baseband.
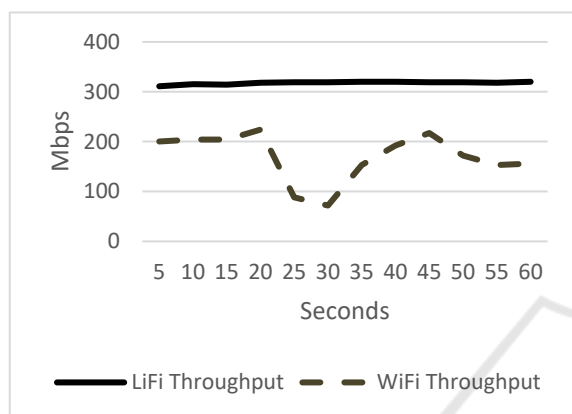

Figure 2: Graph illustrating comparison between LiFi and WiFi performance in pureLiFi's LiFi enabled mobile phone. Tests conducted in typically congested network environment, sampled at 5 second intervals.

Light can be easily contained, and LiFi systems are designed to provide a well-defined area of coverage that does not interfere with neighbouring networks. This allows LiFi networks to exist almost in isolation even in heavily crowded environments. This isolated nature of the network allows it to be immune to ambient radio interference and deliver ultra-low latency connections with a throughput that is highly consistent. For this use case and so many others, LiFi delivers wire-like connectivity in a wireless system.

3 PRIVACY IS PARAMOUT

Cybercrime is no longer only a concern for large corporates and national security but a growing and embedded aspect of modern digital culture that has impact on consumer confidence. The CPX 360 survey performed by iQor found that two-thirds (70 percent) of consumers fear lack of adequate security in their home networks could allow hackers to break in to smart devices in their homes (iQoR, 2021).

Alarmingly NetScout also reported that Internet of Things (IoT) devices are under attack five minutes

after they are powered up and are targeted by specific exploits within 24 hours (Netscout, 2019).

In addition, while the latest 5G systems are being deployed to meet increasing data demand, capacity, and communications requirements, they are opening up all new security vulnerabilities. The NSA released a report in which they warned that the exponential increase in IoT devices connecting to 5G networks is only intensifying these vulnerabilities. (Defense.gov, 2021).

When it comes to security, consumers, employers and industry are increasingly concerned about cyber threats of the kind that LiFi can prevent or mitigate in ways that RF cannot. LiFi provides inherent military grade security while offering robust, fast and reliable wireless communications. LiFi signals are not accessible outside of a defined room or space, because LiFi does not pass-through walls and can be designed to be highly directional. LiFi can also be contained to a defined cone of light. This unique quality of LiFi means that communications are inherently secure providing *intentional* connectivity.
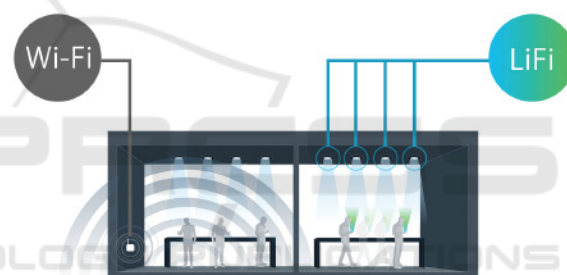

Figure 3: WiFi vs LiFi Networks. WiFi leaking through walls. LiFi contained. ©pureLiFi.

In contrast WiFi and other RF signals are susceptible to eavesdropping from outside. As the FBI warned in a Tech Tuesday bulletin on the risk of smart TVs, "At the low end of the risk spectrum, they can change channels, play with the volume, and show your kids inappropriate videos. In a worst-case scenario, they can turn on your bedroom TV's camera and microphone, and silently cyberstalk you." (Doffman, 2020).

3.1 Unprecedented Privacy for Home Working

Researchers at Cardiff University and Southampton University (Felstead & Reuschke, 2020) showed that 43% of the working population in the UK was working from home by April 2020 as lockdowns came into force, an eightfold increase from January 2020. And, of course, those workers were

continuously accessing networked company resources.

As lockdowns eased in June 2020, the researchers found that (Felstead & Reuschke, 2020) the proportion of homeworkers naturally fell, but only to about 37%. That's an early indicator that much increased homeworking is here to stay even after the pandemic. However, according to OpenVPN 54% of IT managers consider remote workers to be a greater security threat. (OpenVPN)

There is a growing need for secure, high bandwidth and reliable communications in the home office that is simple to implement. LiFi systems are plug and play and are able to complement existing WiFi and network infrastructure in the average home. Self-contained LiFi systems can be provisioned by employers for their home workers that allow only wireless access to networked company resources via a secure LiFi link.
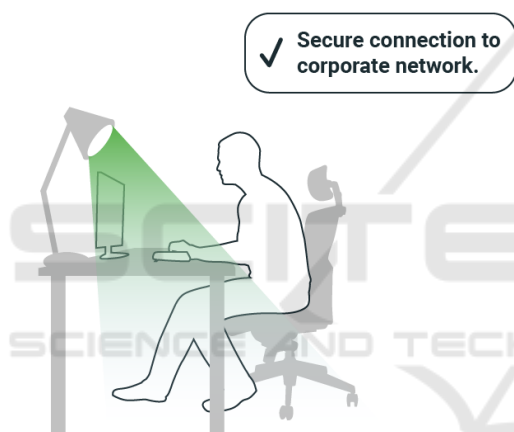
Figure 4: Home worker using self-contained LiFi system for connection to a company network.

Additionally, these unique LiFi access points can be optimised to allow various levels of secure access to information making information management less complex. For example, LiFi link type "A" allows for "Y" security level access and LiFi link "B" allows for "X" Security level access.

If home working is going to remain a new normal, then appropriately securing the employee's home office is essential and LiFi offers a military grade security solution with low logistical impact. Employers can now provide the tools to insist that employees not only use approved company equipment such as laptops and tablets, but they can insist and enforce the use of approved wireless networks at home.

3.2 Intentional Connectivity

While LiFi is a mobile wireless technology it can also offer benefits when used as a point-to-point link. Smartphones are increasingly being used to replace our wallets and our keys while also containing our most sensitive of data such as contacts, banking information, location data, and all of our private videos and photos. It's natural that we also then need to use our phones to not only share sensitive data but to pay for items at shops or to open the doors to our cars and even our homes. The technologies currently used for these types of exchanges and transactions are RF based such as NFC and Bluetooth. Not only are they low bandwidth but they are also vulnerable to eavesdropping and interception. LiFi allows for the implementation of "intentional connectivity" meaning that connections are only initiated when in "line of sight" to the intended recipient. LiFi connections cannot be passively hacked when a phone is in a pocket or handbag, meaning that LiFi exchanges from a phone have a very low probability of interception or attack.

Figure 5: Two of pureLiFi's LiFi enabled mobile phones sharing files securely.

This has secure applications for payments, digital keys or passes and general phone to phone or phone to anything secure data transfers.

4 CONCLUSIONS

Today there are 8.1 billion mobile subscriptions and we consume globally 72 exabytes of data per month and growing (Ericson 2021). While LiFi may not be in every device and every light yet, LiFi components are ready to be designed into the next generation of mobile devices and mainstream access points.

The requirement for LiFi is clear the demand for digital connections is exploding, cyber threats are increasing and industry cooperation is growing, all while RF spectrum congestion isn't getting any bigger. All signs point to LiFi and LiFi is ready.

REFERENCES

Grijpink, Ferry, et al. Connected world: An evolution in connectivity beyond the 5G revolution. McKinsey & Company. [Online] February 2020. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution.

Scrogill, Tim. Is LiFi the Future of Secure Networks? ScureWorld. [Online] 11 September 2017. https://www.secureworldexpo.com/industry-news/is-lifi-the-future-of-secure-networks.

Venugopal, Vineeth. The light way to 6G. SPIE: The International Society for Optics and Photonics. [Online] 1 January 2021. https://spie.org/news/photonics-focus/janfeb-2021/light-way-to-6g.

Pool, Rebecca. LiFi: Coming to a factory, a school, and a car near you. SPIE: The International Society for Optics and Photonics. [Online] 1 Janaury 2021. https://spie.org/news/photonics-focus/janfeb-2021/lifi.

Conviva, [online] 2020, https://pages.conviva.com/rs/138-XJA-134/images/RPT_Conviva_SoS_Q4_2020.pdf

Popular Mechanics [online] February 2015, https://www.popularmechanics.com/flight/a13967/lockheed-martin-augmented-reality-f-35/

Schofield, Jack. Scottish school claims world first for using light-based Li-Fi networking. ZDNet. [Online] 31 August 2018. https://www.zdnet.com/article/scottish-school-claims-world-first-for-using-light-based-li-fi-networking/.

iQoR, [online] 2021, November 2021, https://blog.iqor.com/do-consumer-smart-home-security-fears-outweigh-the-potential-of-the-connected-home-reality-1

Netscout, [online] 2019, November 2021, https://www.netscout.com/sites/default/files/2019-07/SECR_010_EN-1901%20%E2%80%93%20NETSCOUT%20Threat%20Report%201H%202019%20%E2%80%93%20Web.pdf

Defense.gov, [online], 2021, Potential Threat Vectors to 5G infrastructure, 2021 https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

Doffman, Zak. [online], 2020, FBI 'Drive-By' Hacking Threat Just Got Real: Here's Why You Should Be Concerned. Forbes. [Online] 7 October 2020. https://www.forbes.com/sites/zakdoffman/2020/10/07/fbi-drive-by-hacking-threat-gets-real-heres-why-you-should-be-concerned/

Felstead, Alan and Reuschke, Darja. Homeworking in the UK: before and during the 2020 lockdown. Cardiff: Wales Institute of Social and Economic Research.

OpenVPN [Online], https://openvpn.net/blog/remote-workforce-cybersecurity-quick-poll/

Ericson [Onilne[, Auguust 2021, https://www.ericsson.com/assets/local/reports-papers/mobility-report/documents/2021/emr-q2-2021-update.pdf