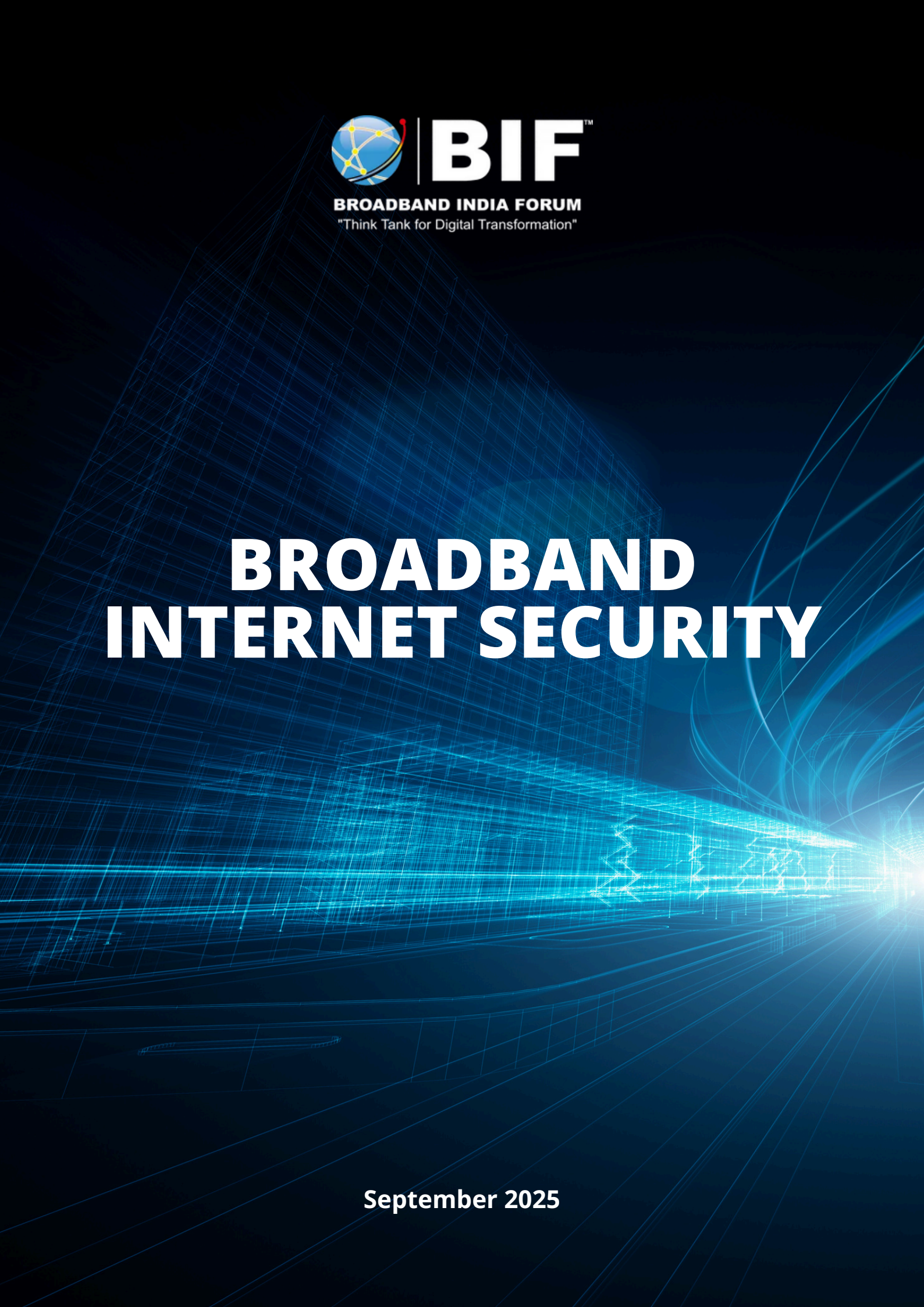

BIF
BROADBAND INDIA FORUM
"Think Tank for Digital Transformation"
BROADBAND
INTERNET SECURITY
September 2025

BROADBAND INTERNET SECURITY

P. V. Ananda Mohan and N. Sarat Chandra Babu

September 2025

Published by

BROADBAND INDIA FORUM
"Think Tank for Digital Transformation"

CONTENTS

EXECUTIVE SUMMARY

The internet or broadband connection has become an indivisible part of modern-day life. Internet security, or cyber security, is a selection of security measures that are implemented to protect any online activities or transactions. Security measures are in place to protect and prevent users from online threats including identity theft, hacking (via email addresses, websites and computer systems) and malicious software attacks. In the case of the internet, we have to deal with malware including *viruses, adware, phishing, spam, spyware, Trojan horses etc.* Hence, it is common to use basic web security software in place from companies such as Norton and McAfee which can include anti-virus and anti-spyware features, as well as a firewall which is used to block viral attacks.

Several options are available for home users, enterprise users, mobile device users to communicate on internet. These include various media such as satellite, coaxial cable, Digital Subscriber lines, Optical fibres and WiFi. In the past few decades, security has been extensively addressed and based on experience learned, continuous evolution of standards has taken place. As an illustration, WiFi security started with WEP and evolved as WPA, WPA2 and more recently as WPA3 and attacks also have become more sophisticated and hence continuous development of standards to remedy the observed problems are evolving However, more awareness about the underlying technologies, security options and measures is believed to be more helpful in protecting the user information from attacks. This white paper addresses the security aspects for the various types of communications - Satellite-based internet, use of DSL, internet over optical fiber and coaxial cable, and WiFi security. We also briefly consider emerging Quantum technologies for Quantum key distribution and post-quantum cryptography algorithms, together with applications in 5G/6G and Access networks. We also describe briefly the application of Quantum technologies in SDN (Software Defined Networking) and NFV (Network Function Virtualization) based networks.

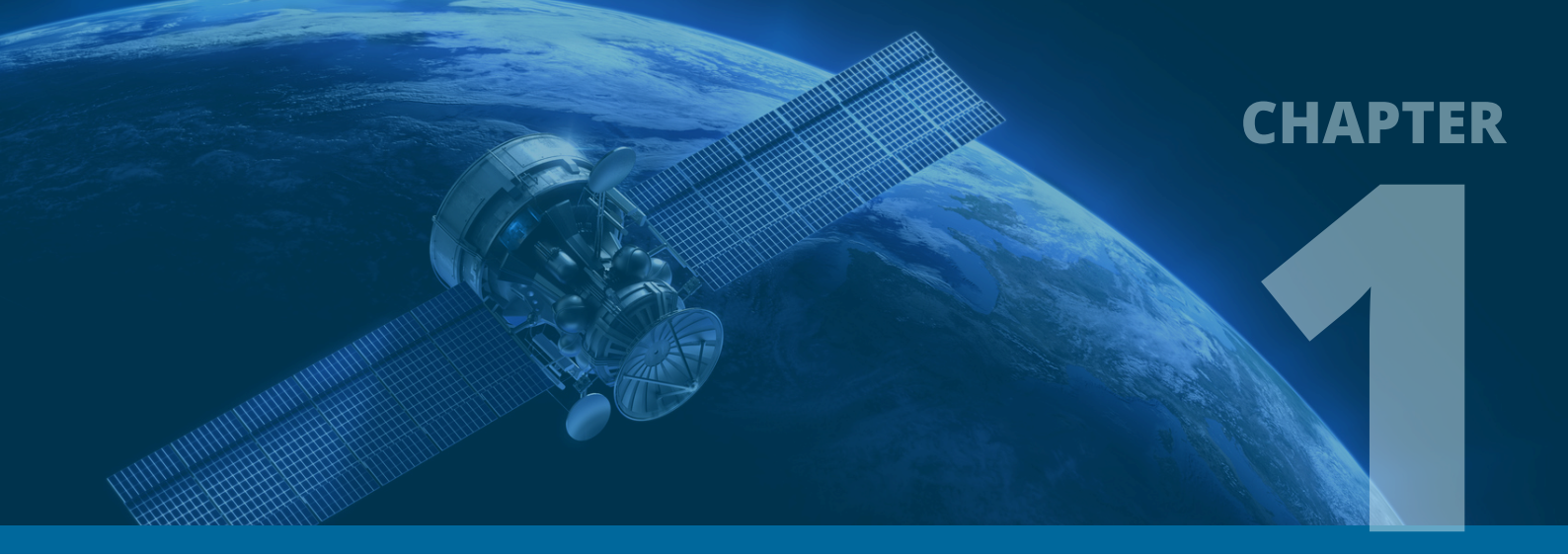
The paper also presents the various technological developments in the various media used for internet access mentioned above, attacks that need to be taken into account as well as remedial measures. We feel that the information presented will help Broadband Internet service providers to be aware of the security concerns and alert the users about precautions to be taken, provide patches to the users as quickly as possible to give assurance regarding cybersecurity. References are also provided to enable the readers of the white paper to consult them for more information.

INTRODUCTION

The Internet user base has been steadily expanding.. The number of non-active internet users is on the decline, but around half of rural India are still not active. Urban India spends slightly more time on the internet per day on average than rural India. Further, video and audio OTT consumption is the top way Indians are using the internet. One in five netizens watch video only over the internet and not on linear TV.. There is an increase in use of non-traditional devices like smart TV, smart speakers, Firesticks, Chromecasts, bluray and gaming consoles. One in four online shoppers in urban India have shopped from social media apps in the past year. Only 26 per cent of online shoppers avail cash on delivery. Music streaming users saw an eight per cent Y-o-Y growth. Digital is now the go-to to access news, but not everyone is a conscious user. One in four urban users are going for voice commands. Indic for India - local language use is taking off across activities. Some languages are found to do better than others.

The internet or broadband connection has become an indivisible part of modern-day life. Internet security, or cyber security, is a selection of security measures that are implemented to protect any online activities or transactions. Security measures are in place to protect and prevent users from online threats including identity theft, hacking (via email addresses, websites and computer systems) and malicious software attacks

In the case of the internet, we have to deal with *viruses* which come in different sneaky forms. The general term virus is also often used, like malware, and it really applies to anything that can infect a programmable device. It is usually destructive. Another type *adware* is not that malicious, but it will trouble us with ads, pop-ups and targeted promotions which will slow your computer and test our patience. Next threat is *malware*, which is specifically designed to cause mild to severe devastation inside the web-connected device, or it could be used to access a private system. The next well-known problem is *phishing*, which involves sending scam emails claiming to be from a known contact, which will request personal details like a PIN, in order to use for fraud. *Spam* is not so much a threat as a nuisance, and is also known as junk mail. Some email providers offer a junk filter, so that this rubbish gets removed before you are bothered by it. Next, *spyware* can help someone to keep tabs on our web activity which operates in secret, and can see personal information entered online. The aptly named *Trojan horse* programs go up to other programs and enthusiastically latch on to them. They wait there until we are really comfortably streaming what you like to watch online, and unleash a torrent of chaos. Hence, it is most essential to have basic web security software in place from companies such as Norton and McAfee which can include anti-virus and anti-spyware features, as well as a firewall which is used to block viral attacks. It's worth checking to see if our broadband provider offers anti-virus software as part of the deal.



CHAPTER 1

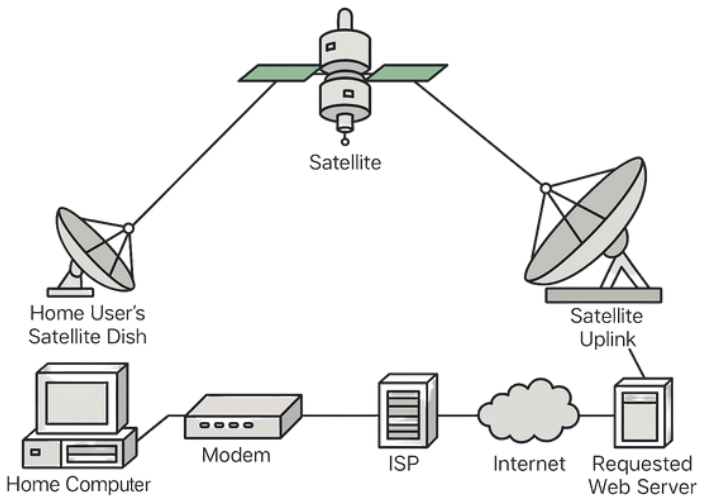
SATELLITE INTERNET

Satellite internet works by using radio waves to communicate with satellites orbiting the Earth. Data is sent and retrieved through a communication network that starts with the user's device and travels through user's modem and satellite dish, out to a satellite in space, then back to Earth to ground stations known as network operations centers (NOC). And then, data travels back through this network—out to space and then back to the user's satellite dish on Earth—to deliver data on his/her device. It is possible get Wi-Fi through a satellite internet connection.

Satellite internet speeds range from 12–100 Mbps, which is enough speed for common online activities like emailing, browsing, and online schooling.. Earlier Satellite internet, primarily based on GEO sats, was not good for fast-paced gaming because it has high latency which leads to an extra delay any time which the user is requesting or sending data. LEO and MEO constellation based satellite internet provides high speed internet at lower latency. However, much like different types of broadband, the *quality of service* (QOS) can depend on a number of factors viz., (a) the number of satellites in orbit**,** (b) distance from the Earth, (c) the transmission technology (d) reliability and (e) availability. Satellite internet is available almost everywhere, making it ideal for rural areas without cable or DSL access. Further, the installation is relatively straightforward with a satellite dish.

Satellite internet uses five components: Internet-ready device, Modem/router, Satellite dish, satellite in space, Network Operations Center (NOC). Some satellite internet modems come with a router built in. The router connects to the modem to give it Wi-Fi capabilities (see Fig.1).

Fig.1 Satellite broadband internet system architecture



The vulnerabilities in satellite systems can manifest in various ways, from exploiting software vulnerabilities in ground control systems to physically tampering with the satellite hardware. Potential risks associated with satellite hacking include unauthorized access to sensitive data, manipulation of satellite functions, and disruption of communication services. Any systems which rely on outdated software or insufficient security protocols, provides avenue for exploitation. Moreover, the lack of regular software updates in orbiting satellites exacerbates the challenge of securing these systems.

Earlier, data transmitted via satellite communication channels were also susceptible to interception by adversaries, posing a significant threat to privacy and national security. Cybercriminals employ techniques like eavesdropping on satellite communication channels and exploiting weak encryption protocols to intercept sensitive data transmitted via satellite. Effective encryption protocols and secure communication channels are imperative to thwart data interception attempts. Advancements in satellite communication security include the implementation of *quantum-resistant encryption* algorithms and the development of *secure key exchange protocols* to counter emerging threats. However, challenges persist in the integration of these technologies due to the resource constraints on satellites and the need for standardized security measures and best practices. Satellite jamming and denial-of-service (DoS) attacks can present tangible threats to the reliability and availability of satellite services. This may lead to disrupting telecommunications and navigation systems, impacting critical infrastructure and national security. To mitigate the risks posed by satellite jamming and DoS attacks, recent advancements in anti-jamming technologies involve the integration of adaptive beamforming, frequency agility, and artificial intelligence to enhance the resilience of satellite systems against intentional disruptions.

Satellite cyber security faces significant challenges, particularly with the proliferation of smallsats by commercial entities like SpaceX's Starlink[1], introducing vulnerabilities. Hence, the proposed solutions include implementing stronger encryption, such as quantum encryption, advancing laser-based communication, and reinforcing intrusion detection (IDS) and prevention systems (IPS). Starlink has average download speeds of between 50Mbps and 300Mbps. Even in the satellite systems there can be potential vulnerabilities that hackers could exploit And a fault injection attack could be carried out, bypassing security measures and gaining unauthorized access to its systems[2]. A new malware, "Malware 4. STL," which utilizes a person's mobile device to remotely gather data on satellite systems, representing a distinctive threat compared to previous concerns about direct hacking or system disruption was recently found. The vulnerabilities in satellite broadband internet networks mentioned above are (a) eavesdropping (b) false signals -injection of deceptive commands or data to disrupt operations (c) Physical attacks on ground stations and (d) unauthorized access. The challenges involved are as follows: (a) Geographical spread (b) traffic monitoring complexities across vast areas (c) system complexity due to various subsytems (d) regulatory hurdles and finally (e) advanced threat landscape – state sponsored attacks.

Counter measures deployed: Ground stations serve as critical points in securing satellite data transmission both uplinks and downlinks of satellite communication by implementing encryption and authentication measures. Encryption algorithms like Advanced Encryption Standard (AES) using key sizes of 128, 192, or 256 bits, and Rivest-Shamir-Adleman (RSA) and Quantum Encryption, quantum key distribution ensure between ground stations and satellites, thus maintaining the confidentiality and integrity of the data being transmitted. Advanced encryption technologies like homomorphic encryption and secure multi-party computation further strengthen security in satellite networks. Implementing advanced encryption protocols like SSL/TLS, IPSec and DTLS enhances satellite network security. Secure communication in satellite networks relies on cryptographic key exchange protocols

like Diffie-Hellman Key exchange. These protocols facilitate the generation of encryption keys shared between satellites and ground stations, ensuring that data transmissions remain confidential and protected from eavesdropping or tampering.

Integrating sophisticated threat detection systems enhances the overall security posture of satellite networks. Additionally, the adoption of Software-Defined Networking (SDN) in satellite systems enables centralized control and monitoring, enhancing overall security by allowing for dynamic security protocol updates and rapid threat responses. Thus, makes internet access using Satcom safe and secure.

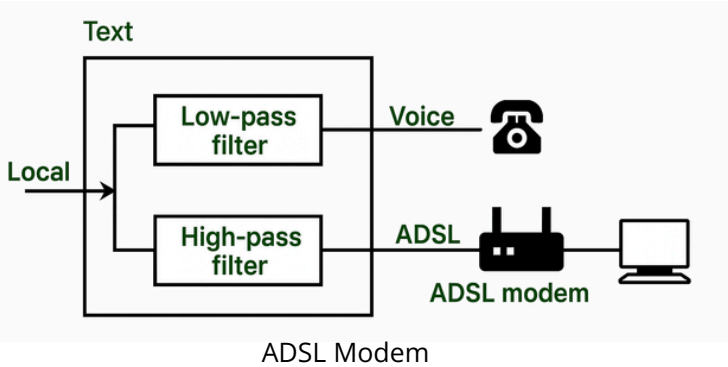
CHAPTER 2

DIGITAL SUBSCRIBER LINES (DSL)

DSL takes advantage of existing copper phone lines to deliver data to the home even at rural areas. And, unlike dial-up, you can still make calls while using the internet. These can carry voice as well as data. Secondly, these offer dedicated connection and hence speeds are not affected by neighbourhood traffic. However, there are disadvantages viz., being generally slower than cable and fiber optic lines. Moreover, the distance from the ISP's central office can affect speed and quality. DSL plan speeds can range from 1 Mbps (practically unusable), to 25 Mbps (enough for surfing and light streaming), up to 100 Mbps (fast enough for multiple people to surf and stream simultaneously). DSL may also be subject to network congestion, meaning we could experience slowdowns during peak hours. The upload speeds will also be much slower than the download speeds, which could be an issue with video calls. At the ISP central office, several DSLs terminate and these are aggregated using DSLAM (DSL Access Multiplexer), which connects to the internet after separating voice and data. The DSL connection at the customer and ISP premises is shown in Fig. 2(a) and (b) for illustration.

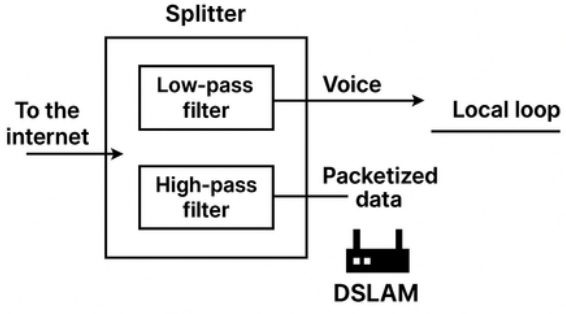
Fig.2. DSL connection at subscriber end (a) and at other end (b).

(a)



ADSL Modem

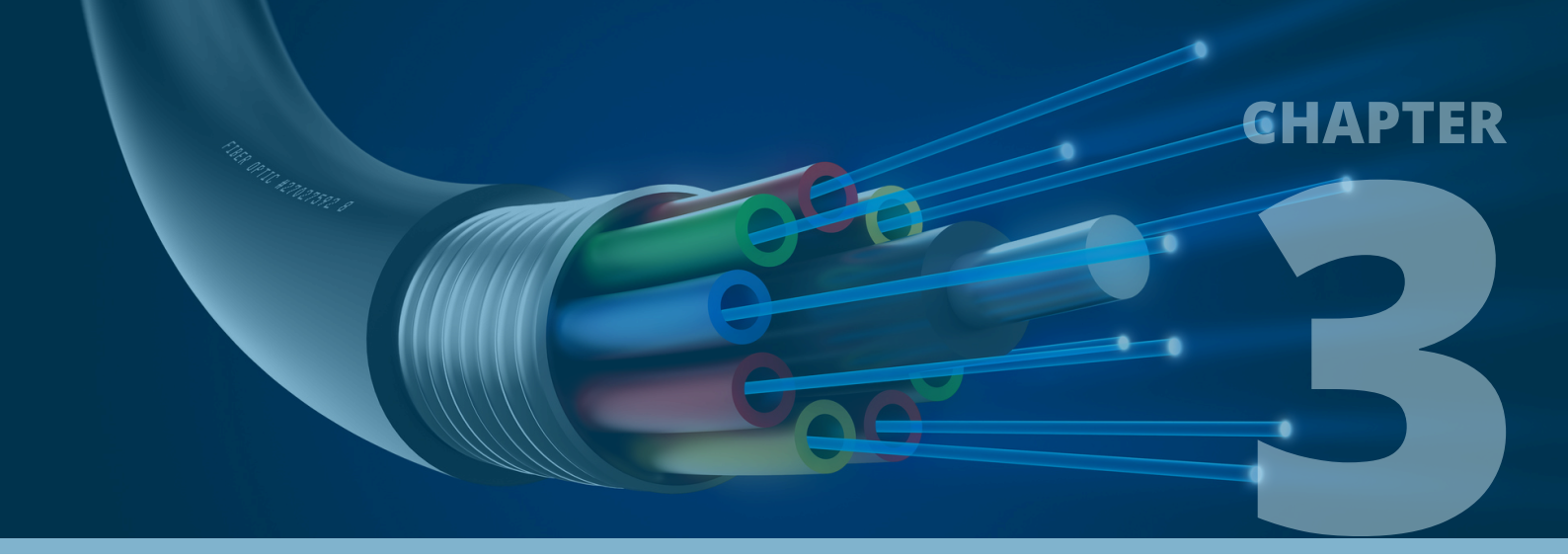
(b)



DSLAM

There are typically 5 types of DSL internet: Asymmetric DSL (ADSL), Symmetric DSL (SDSL), High-bit-rate DSL (HDSL), Very High-bit-rate DSL (VDSL), and Single-pair High-speed DSL (SHDSL). ADSL is primarily designed for residential use and provides faster download speeds compared to upload speeds. SDSL offers equal upload and download speeds. HDSL does not typically support voice data along with internet access. VDSL offers high data rates over short distances whereas SHDSL provides equal upload and download speeds over a single pair of copper wires.

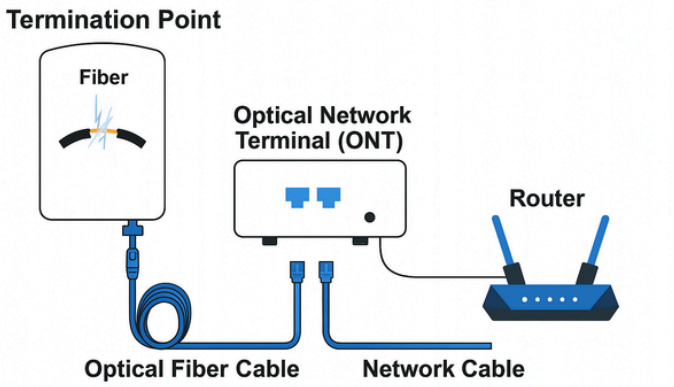
Some ADSLs are available with router function and other features such as parental controls (Web site filtering for all connected devices), VPN support (Secure access to your home network) and Guest network Access—Separate and secure access for guests.



FIBER OPTIC INTERNET

The connection is entirely serviced with fibre optic cables from the exchange to street cabinet and from street cabinet to home (see Fig.3). The advantages of fibre optic internet are fastest internet speeds often up to 1 Gbps or more and also symmetrical upload and download speeds. These are less susceptible to congestion, ensuring consistent performance. However, the limitations are limited availability, as it requires specific infrastructure and further, installation can be more complex and might require digging and also more expensive than other options. These use optical network terminal (ONT) instead of a modem.

Fig.3. Optical fibre based broadband internet system



Fibre broadband security

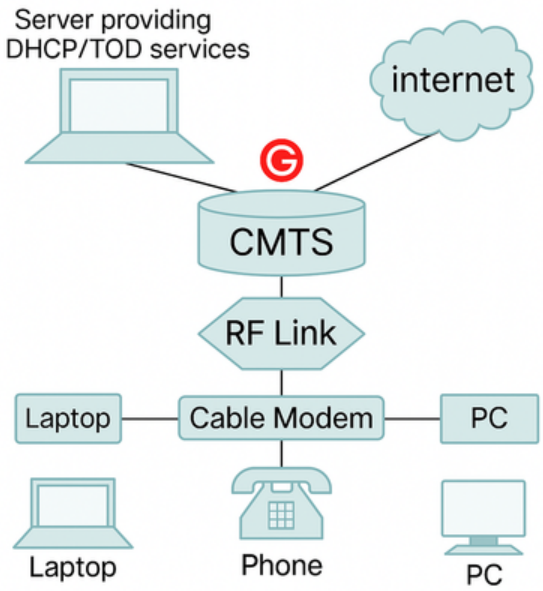
Note that hacking fiber network is also possible. Unlike copper cables, fiber optic cables tend to break easily when they are bent by miscreants. This makes it easier to set an alarm system for identifying a tap into the system. There are different types of transmission encryption methods followed based on the optic fiber infrastructure available. Physical monitoring of the cabling would be the most reliable step since some hackers only need a slight light leak in the cable to gain access into the network. Some even utilize sensors that can accurately capture power changes. This helps in the early identification of network hacks so that major data loss can be averted. Besides the various fiber security measures any ISP integrates in the network, consumers or end users should ensure that the recommended firewalls are turned on. A reliable router with the latest security updates installed should also be at the crux of the network. The Indian government launched the National Broadband Mission in 2019 with an investment of $100 billion, including $35 billion for telecom towers, $30 billion for optical fiber infrastructure, and $35 billion for spectrum and research and development[3].

CABLE INTERNET

Coaxial cables are supehighways that carry internet signals over large distances[4] which typically consist of coper wire surounded by insulating dielectric, an outer metallic shield and a jacket to prevent from moisture etc. This special design protects the internet signals from interference. RG-6 (Radio guide) is one of the recent types used. It is thin and easy to bend. It is possible to add signal boosters for covering large distances. Data to be sent is encoded and modulated for efficient transmission. Several techniques are used like error correction, equalization, signal boosting. This is how data centers are connected to homes.

This needs a cable modem at the user's premises and a cable modem termination system (CMTS) at the cable operator's facility (also known as head-end) and connected to Internet.These two components are connected via a hybrid fibre-coaxial (HFC) network, which combines the benefits of both coaxial cables and optical fibers to provide bi-directional flow of IP data between cable modem and CMTS over hybrid-fiber/coax cable systems (see Fig.4) . From the modem, one can either use an Ethernet cable to directly connect to a computer, providing a wired connection, or connect to a router. The router then broadcasts a Wi-Fi signal, allowing multiple devices in the home to access the internet wirelessly.

Fig.4. System diagram showing Cable modem, CMTS and user premises equipment



While cable internet can offer speeds ranging from 30Mbps to 1,000Mbps, the actual speed can vary based on network congestion, especially during peak times. Further, limited rural availability is a concern as well as cap on the data limits, with fees for exceeding them.

The cable broadband follows DOCSIS (Data Over Cable System Interface Specification)[5],[6], which defines the interface specifications for cable modems. The early DOCSIS versions---DOCSIS 1.0, 1.1, and 2.0, had a basic two-channel design with one channel dedicated to the download and one to the upload. Note that DOCSIS 3.1 could facilitate upload 1-2G b/s and downstream 10Gb/s. DOCSIS 4.0, an enhancement of DOSIS 3.1 introduced in 2019, could have upload at 6G b/s and downstream at 10Gb/s. DOCSIS 4.0 also realized full duplex DOCSIS (FDX) while offering low latency.

The cable modem and customer premise equipment (CPE) requires patches and updates. Cable modem security specifications support SNMPv3 and TR-069, which provide commercial-grade security and include methods for authentication, authorization, access control and privacy in the configuration of devices. In the case of cable equipment, the firmware for these devices can be updated through a special secure channel by the network operator and the firmware image is digitally signed by both the cable modem manufacturer and the network operator.

DOCSIS security

The digital keys used in the cable public key infrastructure (PKI) are based on RSA (Rivest-Shamir-Adleman) 1024 or RSA 2048, that are unique to each cable modem and part of each cable modem's digital certificate. The Baseline Privacy Interface in DOCSIS 3.0, adds support for 128-bit Advanced Encryption Standard (AES). The BPI/SEC specifications describe MAC layer security services for DOCSIS CMTS to cable modem communications. BPI/SEC provides (a) cable modem users with data privacy across the cable network and (b) the cable service operators with service protection (i.e. prevent unauthorized modems and users from gaining access to the network's services). Further, BPI/SEC prevents cable users from listening to each other. It does this by encrypting data flows between the CMTS and the cable modem using TEK (Traffic encryption Key). Note that the use of AES is optional and depends on the cable operator activating it. Note that BPI+ encrypts only DOCSIS MAC Frame's packet data; and the MAC Frame's Header is not encrypted.

In case of BPI+, CMs must have factory-installed RSA private/public key pairs for the increased key sizes (4096 bit for root, 3072 bits for other CAs.

The DOCSIS 4.0 version of the specification introduces new security properties such as full algorithm agility, Perfect Forward Secrecy (PFS), Mutual Message Authentication (MMA or MA) and Downgrade Attacks Protection and improved security for network credentials such as private keys. The new authentication framework requires both parties to participate in the derivation of the Authorization Key from authenticated public parameters. BPI+ V2 uses the Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) algorithm for deriving the authentication key. With foresight of emerging advancements in classical and quantum computing, algorithm agility is also permitted. DOCSIS 4.0 security protocol effectively decouples the public key algorithm used in the X.509 certificates from the key exchange algorithm. This enables the use of new public key algorithms when needed for security or operational needs like in Post-Quantum scenario. DOCSIS 4 also gives support for TLS (Transport layer encryption). The downgrade attack protection is met using Trust On First Use (TOFU) mechanism. It leverages the security parameters used during a first successful authorization as a baseline for future

ones, unless indicated otherwise. By establishing the minimum required version of the authentication protocol, DOCSIS 4.0 cable modems actively prevent unauthorized use of a weaker version of the DOCSIS authentication framework (BPI+).

The Indian government launched the National Broadband Mission in 2019 with an investment of $100 billion, including $35 billion for telecom towers, $30 billion for optical fiber infrastructure, and $35 billion for spectrum and research and development. A further $13 billion investment was announced in 2023, aimed at developing India's optical fiber grid.

CHAPTER 5

WIFI SECURITY

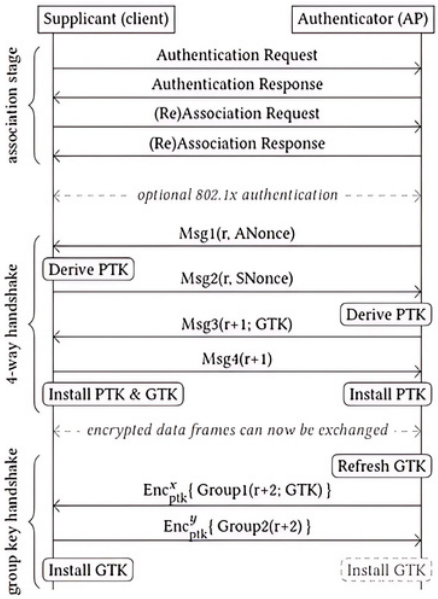
A technique known as Wired Equivalent privacy (WEP) was the first version which has used a stream cipher using RC4 algorithm[7] using a key of 40 bits or 104 bits and an initialization vector (IV) of 24 bits makes up overall key of 64 bits (or 128 bits). Note that initially the WiFi device and access point (AP) have preshared key installed. All the WiFi devices share the pre-shared key (PSK) with the AP. Several attacks such as collision attack, chop-chop attack are available openly in *Aircrack-ng* and *John the Ripper*.

The next generation Wi-Fi protected access (WPA)[8] also was shown to be vulnerable for attacks and was replaced in Wi-Fi Protected Access (WPA2) protocol which uses stronger AES-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) encryption algorithm. WPA2-PSK needs proper passphrase at least 16 characters so that the time needed to crack that password is measured in decades, not hours.

Note that WPA-2 is available in two modes: WPA2-*personal* and WP2-enterprise. Note that the WPA2-*personal* uses pre-shared key discussed above. On the other hand, deploying WPA2-Enterprise requires a RADIUS (*Remote authentication dial-in user service*) server (also called AAA (Authentication, Authorization and accounting) server). Note that X.509 digital certificates are used for authentication[9]. WPA2 Enterprise requires an 802.1X authentication server.

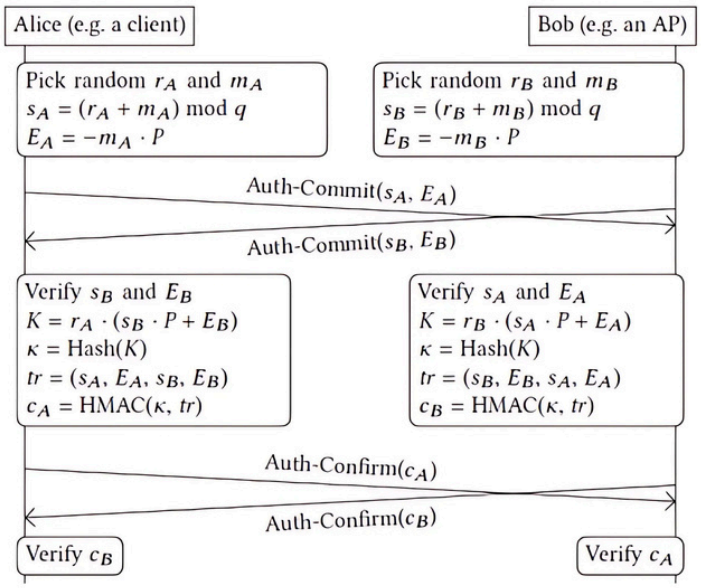
WPA2 uses four-way handshake shown which needs the existence of Pre-Shared Key (PSK) without actually transmitting it. During this handshake, a Pairwise Transient Key (PTK) and Groupwise transient key (GTK) are generated for secure data exchange using MAC addresses, nonces and SSID (Service set identifier which can be seen in the mobile by selecting WiFi settings). Key reinstallation attack (KRACK) was discovered forcing nonce reuse[10] (see Fig.5) . The KRACK attack can be remedied by checking whether key already in use is being reinstalled. The replay counters and nonces shall not be reset. Some patches have been released and are available.

Fig.5. Four-way handshake used in WPA2



Since WPA2 which was in use for over a decade, WPA3 was introduced in 2018 which solves the problem of offline dictionary attack. WPA3 has two methods: WPA3-SAE, or *Simultaneous Authentication of Equals*. Note that SAE uses *dragon fly Key exchange*[11](see Fig.6) and is more resistant to offline dictionary attacks. The end user will not notice any difference since he/she still enters a passphrase on his/her device to secure their Wi-Fi Connections. WPA3-SAE uses *Elliptic Curve Cryptography* (ECC) without needing to send any part of the keys over the air that attackers can capture and then reverse engineer. Note that pairwise master key is based on random numbers and not passwords alone. WPA3 uses AES- CCMP (counter mode with cipher block chaining) and has *forward secrecy* feature which prevents decryption of previous sessions in case current keys are compromised. However, just like with previous generations, not every device today supports WPA3. WPA3 is backward compatible with WPA2 as well as mixed mode WPA2/WPA3 devices.

Fig. 6. SAE handshake used in WPA3



Note that *WPA3 Enterprise* version allows individual keys for each user of 192 bits and uses authenticated encryption based on AES –GCMP (Galois counter mode protocol). It also uses 384 bit HMAC (Hashed Message Authentication code) using SHA 384. The key establishment uses 384 bit ECDH (Elliptic Curve Diffie-Hellman key exchange) for key establishment and authentication uses ECDSA (Elliptic Curve Digital Signature Algorithm).

Several versions of WPA3 are available (a) WPA3 transition mode (b) WPA3 Easy Connect (c)WPA3 Certified enhanced open and Opportunistic Wireless Encryption.

Attacks on WPA3

Since the PMK derived for WPA3 is not solely dependent on passphrase but also needs the random scalar and Finite Field Element, WPA3 helps mitigating Offline dictionary attacks where an attacker uses a dictionary of passphrases on a passively observed WPA3-Personal key exchange to obtain the correct passphrase. Even if the attacker was able to obtain the correct passphrase, it only works for the particular session and not other sessions as the PMK changes for other sessions with random numbers used in generating of scalar and Finite Field Element. Other attacks possible are Denial of Service (DoS) Attacks and Disconnect Attacks. WPA3 uses Protected Management Frames which enforces the encryption of frames and enables APs and clients to detect forged disconnect frames and ignore them. Other attacks possible are *Honeypot and Evil-Twin Attacks and WPA3 Dragonblood attack. D*ragonblood[12],[13] includes a denial-of-service attack, two downgrade attacks and two side-channel attack information leaks on WPA3 and EAP-pwd. These are timing attacks based on side-channels and cache based. Four of the five (not including the denial-of-service attack) are used to steal user passwords.

The Dragonblood vulnerabilities can be fixed with software patches. Further, one shall use strong passwords on their networks. The client should remember if a network supports WPA3-SAE. That is, after successfully connecting using SAE, the client should store that the network supports SAE. From this point onward, the client must never connect to this network using a weaker handshake. Another defense, which requires no software patches, is to deploy separate WPA2 and WPA3 networks with different passwords.

It is also necessary not to operate in an unlicensed spectrum with a Common Air Interface **(**CAI**)** that opens up many opportunities for attackers to find vulnerabilities.

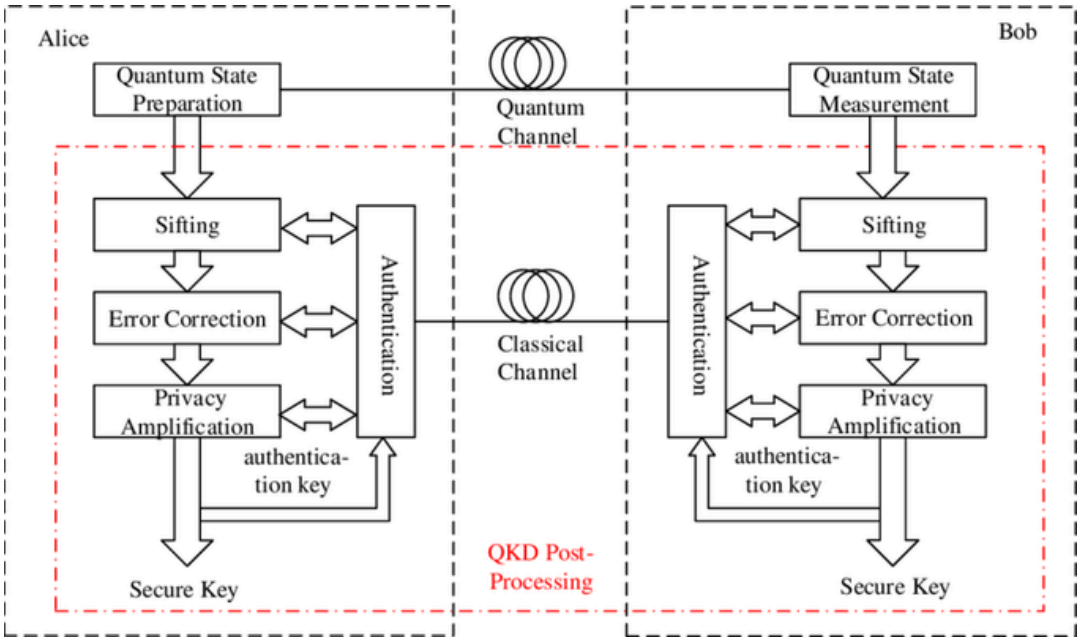
The latest generation of WiFi is WiFi7 which can facilitate Multi link operation (MLO)[14] simultaneously in three different frequency bands 2.4GHz, 5GHz, and 6GHzwith different performance. The band 2.4 GHz used for headless devices, IoT and sensors is latency insensitive whereas 5GHz band used for user interfaced devices, laptops, PCs etc is latency sensitive. On the other hand, 6GHz band is latency critical used in Medical, gaming, financial, AR/VR applications. Note that Wi-Fi 7 routers need at least WPA2 for 5GHz and/or 2.4GHz bands whereas the 6GHz band always requires WPA3. The MLO operation uses multiple bands to simultaneously connect AP and user device. Note that instead of three SSIDs, only one SSID is used. In other words, there is only one high level MAC address which is used to generate the encryption keys; instead of three keys being used (one key for each of the possible radio bands being used), the devices only need to build one set of keys. The standards are still evolving.

QUANTUM KEY DISTRIBUTION AND APPLICATIONS

QKD is a cryptography approach that uses quantum physics to establish a shared secret key between two parties Alice (the sender) and Bob (the receiver). This key is subsequently utilized to encrypt and decrypt messages, guaranteeing the highest level of security. The most common qubits being studied today are quantum dots, ion traps, superconducting circuits, and defect spin qubits. A random bit of data, such as a 0 or a 1, is encoded into the photons. When the photons become available, the parties may analyze them to figure out the encoded bit of information. If an eavesdropper, or and tries to intercept the photons, he/she will invariably perturb them in a way that both parties can notice. This allows the parties to determine if their key was compromised and produce a new key. Qubits are fickle because they are error prone.

There are two types of QKD systems Continuous Variable (CV) that uses wave nature of light and DV (Discrete Variable) that uses particles of light. DV QKD is more popular. There are two major parts in a DV-QKD system: the quantum subsystem and the post-processing Subsystem (see Fig. 7).

Fig. 7. A general structure of a QKD system



The quantum subsystem is responsible of the preparation, transmission and measurement of quantum states. The post-processing subsystem distills Alice and Bob's fully uniform and secure key from their partially uniform and secure strings through a public but authenticated channel. Note that the basis of a qubit can be horizontal or vertical and the polarization also can be horizontal or vertical. In a QKD protocol, Alice sends a series of quantum states (typically individual photons) to Bob over a quantum channel. These quantum states encode the secret key bits. Error correction techniques are employed to detect and correct the errors. After error correction, the remaining errors, known as the "residual errors," need to be eliminated to guarantee the security of the final key. This is achieved using *privacy amplification* which is a process that transforms the initial key using *public discussion* yet containing some residual errors (and potentially be known by an eavesdropper), into a final key that is secure and completely unknown to any adversary. Note that QKD relies on hop-by-hop security between intermediate trusted nodes. The post-processing subsystem mainly includes four parts: authentication, sifting, error reconcilliation and privacy amplification (PA).

Quantum Entanglement

Entanglement QKD leverages one of the more interesting quantum phenomena where two quantum particles are generated in a way in which they share quantum properties and no matter how far apart, a measurement of a property on each will result in the same values. Hence, two entangled photons possessing the same polarization could be measured in two locations, providing the same polarization values. Entanglement QKD is useful towards the realization of a quantum internet. Albert Einstein named this phenomenon as "spooky action at a distance". Qu*antum teleportation* is a process by which the quantum state of one qubit can be transmitted to another qubit without any physical transfer of matter or energy. This process involves the measurement of the quantum state of the original qubit, which destroys the state, and the transmission of classical information about the measurement results to the receiving party, who can then recreate the original quantum state using a third qubit. In order to carry out QKD using entanglement, it is necessary to build the appropriate infrastructure to first create pairs of entangled qubits, and then distribute them between a sender and a receiver. This creates the "teleportation" channel over which cryptography keys can be exchanged. Specifically, once the entangled qubits have been generated, one half of the pair needs to be sent to the receiver of the key. An entangled qubit can travel through networks of optical fibre, for example; but those are unable to maintain entanglement after about 60 miles. Qubits can also be kept entangled over large distances via satellite, but covering the planet with outer-space quantum devices is expensive.

Innovations such as continuous-variable QKD, satellite-based QKD, and chip-scale integration are enhancing the performance and scalability of QKD systems. These advancements address key challenges, such as transmission distance and system complexity, making QKD more viable for a broader range of applications.
QKD products in market

Quantum Key Distribution (QKD) using different protocols BB84/E91/ BBM92[15] protocols, Shor protocol, MDI (Measurement Device Independent)-QKD protocol are of interest. Secondly, QKD systems of various types Discrete-variable QKD, Continuous-variable QKD, Multi-party QKD are also available in market. Multi-party QKD allows multiple people to share a secret password. It is utilized in applications like secure group interaction and quantum voting. In addition Quantum key distribution networks, Quantum key distribution chips, Quantum key distribution software are in demand. Further, various segments such as Government and defence, Finance, Telecommunications, Healthcare, Internet of Things are interested in QKD. Quantum Key Distribution Networks are typically

made up of an array of QKD nodes connected by optical fibres. Quantum Key Distribution Chips allow QKD components to be integrated into smaller and more compact devices. This makes QKD more applicable to a broader range of applications. Quantum Key Distribution Software is used for handling and running quantum key distribution (QKD) devices which comprises key creation, distribution, and encryption capabilities. The following are the emerging applications of QKD (a) Cybersecurity (b) Integration of QKD in 5G/6G Network, : (c) Growing Adoption in Critical Infrastructure Protection, (d) QKD in Cloud Computing and Data Centers(e) Healthcare (f) Internet of Things (IOT) and (g) Quantum Money.

The global quantum key distribution (QKD) market size was US $1428.3 million in 2021 and is expected to reach USD 8899.9 million by 2031, at a compound annual growth rate (CAGR) of 19.3% during the forecast period. The size of the global Quantum Key Distribution market was estimated at US$ 2.10 billion in 2023 and is projected to increase at a CAGR of 22.2% from 2023 to 2030, reaching US$ 7.88 billion. The top QKD companies are ID Quantique (Switzerland), SeQureNet (France), Quintessence Labs (Australia), MagiQ Technologies (U.S.), Toshiba (Japan), QuantumCTek (China), Qasky (U.S.) and Qudoor (China)[16].

Quantum Random number generators (QRNG) are used to generate key with great degree of randomness (entropy). In Quantum RNGs or QRNGs the source of randomness is a quantum process. Using a QRNG as a source of entropy makes a cryptographic system robust against attacks. As an illustration, IDQ's QRNG chip, a QRNG can now be embedded locally, even for the protection of IoT and edge devices.

QKD using Satellite communication

Quantum satellite networking is central to enabling quantum key distribution (QKD) and quantum-state transfer. Satellite QKD[17]can use CV-QKD or DV-QKD. Note that hybrid system using both CV and DV (DV entanglement over CV channel) is also possible.

Quantum internet

The quantum internet[18],[19] involves sending qubits across a network of multiple quantum devices that are physically separated. Quantum internet leverages the *entanglement* property to communicate between two devices. The quantum internet could significantly reduce the risk of cyber threats, such as hacking, phishing, and data breaches. With quantum encryption, any attempt to eavesdrop on a quantum communication would be detected by the parties involved, making it a highly secure method of communication. The entanglement network used for QKD could also be used, for example, to provide a reliable way to build up quantum clusters made of entangled qubits located in different quantum devices. Despite the potential benefits of the quantum internet, there are significant challenges to its development.

Post-Quantum cryptography

Traditionally, Public key cryptosystems were based on RSA (Rivest-Shamir-Adleman) and Elliptic curve cryptography (ECC). The key exchange was using Diffie-Hellman key exchange algorithm. These have been in use for few decades and their strength relied on the difficulty of factorization of big numbers and discrete logarithm problem. Most internet protocols like SSL/TLS, IPSec were using these in Web browsers, routers, mobile handsets etc. The encryption was using AES 128 algorithm. The advent of quantum computers can affect these systems since the use of quantum algorithms like Shor's

algorithm and Grover's technique can solve the mathematically complex underlying difficult problems. The number of qubits required to break 256 bit AES are 6,681 and to break RSA-2048 are 4096 Qubits. Note, however , due to the errors inherent in quantum processes, it is estimated that the number of Qubits required to break 256 bit AES are 334, 050 (= 6,681×50) and to break RSA-2048 are 204,800 (=4096×50) Qubits respectively[20]. Note that an adversary can capture network traffic today in the hope of decrypting it later. This is a *Store Now, Decrypt Later* (SNDL) type of attack (also called *Harvest Now Decrypt Later* (HNDL). *Years to Quantum* (Y2Q) refers to the unknown number of years before there are *Cryptographically Relevant Quantum Computers* (CRQC) which can break RSA etc. As such, considerable research has been carried out in the past two decades to discover new approaches/algorithms. These are based on different mathematical problems. NIST has invited proposals from across the world and after third round Crystals Kyber[21] has been selected for KEM (*Key encapsulation Mechanism*) which is based on Module Learning with Errors problems. For digital signatures, they have selected Dilthium[22] which is also based on *Module Learning with errors* problem and SPHINCS+[23] which is based on Hash functions SHAKE256, SHA-256, and Haraka. Draft standards for these have been released for public scrutiny. The basis of *lattice-based cryptography* lies in the difficulty of solving problems with lattice structures in spaces with a high number of dimensions. FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU) was also recommended by NIST for digital signatures. Note that NTRU stands for "N-th degree Truncated polynomial Ring Units".

Table I. Key and ciphertext sizes (in bytes) for Crystals Kyber

Candidate	Claimed Security	Public Key	Private key	Cipher text
Kyber 512	Level 1	800	1632	768
Kyber 768	Level 2	1184	2400	1088
Kyber 1024	Level 3	1568	3168	1568

Table II. Key and signature sizes (in bytes) for Dilithium, FALCON and SPHINCS+

Candidate	Claimed Security	Public Key	Private key	Cipher text
Dilithium	Level 1	1312	2528	2420
	Level 2	1952	4000	3293
	Level 3	2592	4864	4595
FALCON312	Level 2	897	7553	666
FALCON 1024	Level 5	1793	13953	1280
SPHINCS+128s	Level 1	32	64	7856
SPHINCS+128f	Level 1	32	64	17088
SPHINCS+192s	Level 3	48	96	16224
SPHINCS+192f	Level 3	48	96	35664
SPHINCS+256s	Level 5	64	128	29792
SPHINCS+256f	Level 5	64	128	49856

s= simple, f = faster

The reader may see **Table I and II** for details about key lengths for Kyber KEM and key lengths and signature size comparison for post Quantum digital signature standards of NIST. Note that in place of separate algorithms for key exchange and authentication, KEM is used to implement public key encryption as well as driving a session key for encryption. AES 256 needs to be used for encryption in view of it's resistance to Grover's attack. The key sizes, signature sizes are more for these new algorithms. The algorithms can cater for different security levels depending on the selected options. These are being incorporated in next generation TLS, web browsers, Routers etc. Efficient Implementations on ASIC, FPGA, ARM processors, and GPUs are of continuing interest. Note that the new generation implementations also shall have *side channel resistance*. The communication overhead of the new algorithms could lead to packet fragmentation in network communication, for example. This also applies to the authentication, key generation, encryption and integrity in 3G, 4G and 5G that rely purely on symmetric cryptography.

Quantum Access networks

A metro area Quantum access network (MAQAN)[24] has been set up in India by a consortium of IIT Madras, Society for Electronic Transactions and Security (SETS) Chennai, Centre for Development of Advanced Computing (C-DAC) and ERNET at Centre for Quantum Information, Communication and Computing (CQuiCC) in October 2022 as a test bed for different protocols. Quantum internet with local access is under development. Telecommunication Engineering centre, India has released a STANDARD FOR GENERIC REQUIREMENTS No. TEC 91000:2022 for Quantum Key Distribution System giving details of generic requirements and specifications for Quantum Key Distribution (QKD) systems as per, ITU-T Y.3801-3804 recommendations for use in Indian telecom network. Post Quantum cryptography and QKD are also being considered for application in wireless networks 6G and beyond.

CISCO outlines the future roadmap [20] shall focus on (a) Developing larger quantum computers (currently 1180 Qubits), (b) Achieving longer quantum coherence greater than 343 ms, (c) requiring fewer qubits for error correction (currently 48), (d) extending current entanglement record of 248Km (e) rising operating temperatures now -273°C, (f) achieving longer quantum memory (g) planning and modelling quantum networks (h) developing quantum network protocols and (h) lowering costs.

As a part of National Quantum Mission (NQM), several IITs, IISc and IISER are introducing specialized courses to create talent pool in Quantum technologies- quantum communication, quantum sensing, quantum computing, quantum materials and Quantum algorithms. It appears that VCs are not aware of the potential of these technologies and need to be educated. The start ups have to work with system integrators to develop the applications as well as market for them.

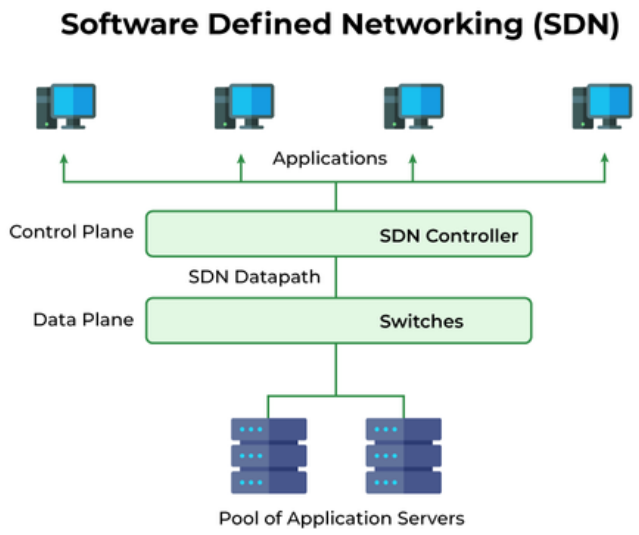
CHAPTER 7

SOFTWARE-DEFINED NETWORKING (SDN)

Software-defined networking (SDN) is a modern approach to managing computer networks by separating the control of the network (the decisions about where data goes) from the actual movement of data in the data plane. This controller has complete visibility and authority over all network activity in a centrally controlled manner through software applications using open APIs for making routing tables and setting packet handling policies. The data plane performs forwarding of packets, Segmentation and reassembly of data and replication of packets for multicasting and is dedicated solely to traffic forwarding, which is performed by executing instructions delivered from the network controller. The data plane still resides in the switch and when a packet enters a switch, its forwarding activity is decided based on the entries of flow tables, which are pre-assigned by the controller. (see Fig. 8 illustrating SDN architecture).

SDN has disadvantage as well, due to the central dependency of the network means a single point of failure, i.e. if the controller gets corrupted, the entire network will be affected. The three interfaces within an SDN architecture to be secured are (a) the northbound interface (NB): from the controller(s) to the orchestrator or application layer, (b) East-westbound interface (EWB) between controllers, and (c) the southbound interface (SB) from the data plane devices to the controllers. SDN can be secured in the control plane using several encryption solutions such as IPsec, Secure Shell (SSH) and transport layer security (TLS).

Fig.8. SDN architecture

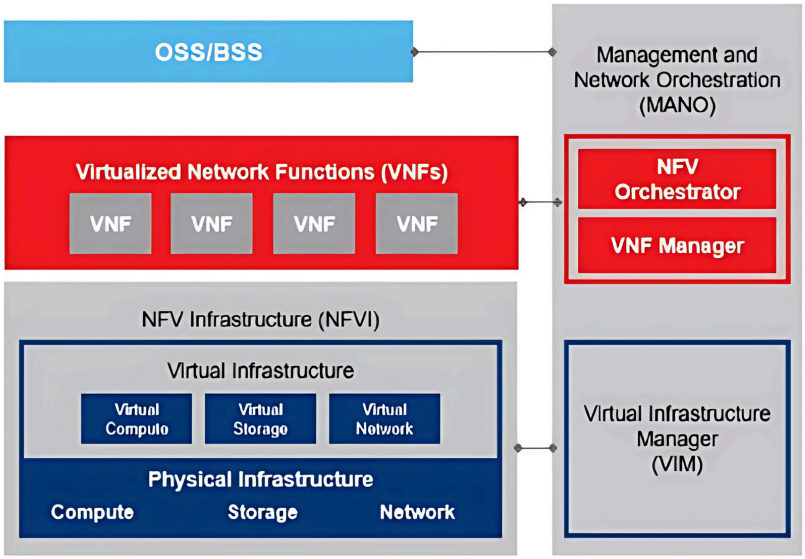


Network Function Virtualization

Network function virtualization (NFV) promises significant network infrastructure simplification as current hardware appliances such as firewalls, Intrusion detection systems (IDS) and load balancers are replaced with software running on standard servers. NFV is complemented by software-defined networking (SDN), provisioning the required network connectivity to respond to newly instantiated appliances by aligning network topologies in an automated manner.

However, there are security risks associated with NFV deployment (see Fig.9). In an NFV enabled network infrastructure, network functions are stored centrally as software images in a remote data center (DC) where they can be cloned, transferred and deployed as virtual functions on commodity servers (replacing network appliances) across the network. This transfer of network functions must be secured, as any attempt to tamper with NFV can create a significant security breach.

Fig. 9. NFV architecture



SDN networks need to integrate a quantum-safe technology of choice as the base for encrypting control plane communications using both QKD and PQC.

The GSMA PQTN Task Force has published an exhaustive document[25] about the impact of Post-Quantum Cryptography (PQC) on telecoms for various use cases. Zero trust architecture (ZTA) in the Post-Quantum era is considered important. The approach for legacy products and services is considered in a phased way to mitigate risk in the appropriate timeframe.

CONCLUSION

In this white paper, we have surveyed the various options available for providing internet over various media and the security issues in those. The normal practices used in IT security need to be continued. At the same time, media specific security awareness is required so that the user is aware of the problems and precautions/ actions to be taken.

There is a need for carrying out research on attacks and counter measures/ fixes/ software patches by creating test beds for various technologies. There is also a need for educating the users about the options available, pitfalls, not allowing use of downgraded protocols etc. The development trajectory of all the standards recommends that more openness while creating the new standards could have prevented most attacks.

REFERENCES

1 Recent Intel Report Reveals New Starlink Vulnerabilities, Increasing Concerns About the Future of Global Satellite Internet - The Debrief, August 15, 2023

2 Chris Young, A hacker used a $25 custom-built tool to hack into SpaceX's Starlink satellite system, Aug 11, 2022

3 Sev Sadura, Looking at the Future of Fiber Broadband in 2024, PPC Broadband, https://www.ppc-online.com/blog/future-of-fiber-broadband-in-2024

4 Lindon Sietz, What is Cable Internet? Everything You Need to Know, BroadbandSearch, https://www.broadbandsearch.net/blog/what-is-cable-internet

5 D. Fellows and D. Jones, "DOCSIS TM cable modem technology," in *IEEE Communications Magazine*, vol. 39, no. 3, pp. 202-209, March 2001.

6 B. Berscheid and C. Howlett, "Full Duplex DOCSIS: Opportunities and Challenges," in IEEE Communications Magazine, vol. 57, no. 8, pp. 28-33, August 2019, doi: 10.1109/MCOM.2019.1800851

7 M. Shin, J. Ma, A. Mishra and W. A. Arbaugh, "Wireless Network Security and Interworking," in Proceedings of the IEEE, vol. 94, no. 2, pp. 455-466, Feb. 2006, doi: 10.1109/JPROC.2005.862322.

8 E. Tews and M. Beck, "Practical attacks against WEP and WPA," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec '09), Zurich, Switzerland, 2009, pp. 79–86.

9 Simplifying WPA2-Enterprise and 802.1x, Secure W2, https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplif...

10 Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In CCS

11 RFC 7664: Dragonfly Key Exchange, RFC Editor, *https://www.rfc-editor.org/rfc/rfc7664.html*

12 Mathy Vanhoef and Eyal Ronen, Dragonblood: Analyzing the {Dragonfly} Handshake of WPA3 and EAP-pwd, in proceedings IEEE Symposium on Security & Privacy (SP),2020

13 Daniel De Almeida Braga, , Pierre-Alain Fouque and France Mohamed Sabt, **Dragonblood** is Still Leaking: Practical Cache-based Side-Channel ..., arXiv.org, *https://arxiv.org/pdf/2012.02745v2* · PDF file

14 Wi-Fi 7 Security: Essential Information You Need, RUCKUS Networks, *https://www.ruckusnetworks.com/blog/2023/wi-fi-7-and-security-wh...*

15 Quantum Key Distribution - William & Mary, wm.edu, *http://cklixx.people.wm.edu/teaching/QC2021/QC-chapter...* · PDF file

16 Quantum Key Distribution Market Size and Forecast to 2030, Coherent Market Insights, *https://www.coherentmarketinsight...*

17 S. Sodagari, "Integrating Quantum and Satellites: A New Era of Connectivity," in IEEE Access, vol. 11, pp. 145101-145110, 2023, doi: 10.1109/ACCESS.2023.3344321.

18 Daphne Leprince-Ringuet , What is the quantum internet? | University of Chicago News, University of Chicago News, *https://news.uchicago.edu/explainer/quantum-internet-explained*

19 T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek and R. V. Meter, "Attacking the Quantum Internet," in IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-17, 2021, Art no. 4102617, doi: 10.1109/TQE.2021.3094983.

20 Tim Szigeti, An introduction to Quantum network technologies, Outshiftby Cisco, *https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/...* · PDF file

21 FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, **Date Published:** August 13, 2024, https://doi.org/10.6028/NIST.FIPS.203

22 FIPS 204, Module-Lattice-Based Digital Signature Standard, **Date Published:** August 13, 2024. https://doi.org/10.6028/NIST.FIPS.204

23 FIPS 205, Stateless Hash-Based Digital Signature Standard, **Date Published:** August 13, 2024,https://doi.org/10.6028/NIST.FIPS.205

24 Anil Prabhakar, Building a Metro Areas Quantum Access Network (MAQAN), quICC, IIT Madras, quantum.iitm.ac.in

25 GSM Association Non-Confidential Official Document PQ.03 – Post Quantum Cryptography – Guidelines for Telecom Use Cases, Version 1.0, 22 February 2024, GSMA, *https://www.gsma.com/newsroom/wp-content/uploads/P...* pp.1-104

BIF™

BROADBAND INDIA FORUM

"Think Tank for Digital Transformation"