Network Security Attacks

With the Internet and new networking technologies computer networks are required in every day communication by individuals, in businesses and government organizations. Attacks on computer network has increased with increasing networks in various businesses and organizations. Network administrators provide security from unauthorized access and risks by adapting preventive measures for network security. Network security is having huge importance due to large personal, commercial, military, government information on networking infrastructure.

Network Security:

Security of computer at transmitter and receiver doesn't mean a complete security. The whole network must be secure while transmitting data through the communication channel. Securing network need to consider:

- Access
- Confidentiality
- Authentication
- Integrity
- Non-repudiation

Attacks on the Networks are as follows:

- Eavesdropping: Interception of communication by unauthorized access is known as eavesdropping. In active eavesdropping, intruder listen and insert something in to the communication signal.
- Viruses: Virus is self-replicated programs used to infect the files and propagate and activated after opening the file.
- Worms: Worms are also self-replicating and of two main types, mass mailing worms and network aware worms.
- Trojans: Trojans are usually carry viruses which appears like a program.
- Phishing: Phishers trick users to disclose the personal data, online banking credentials and other sensitive data.
- IP Spoofing Attacks: The identity of intruder is hidden by various means making detection and prevention difficult.
- Denial of Service: Occurs when system receives too many requests cannot return communication with the requesters.
- Node Subversion: A particular node is captured and keys stored on it might be obtained.
- Node Malfunction: will generate inaccurate data.
- Node outage: is a situation occurs when node stops its function.
- Physical Attacks: physical attacks destroy sensors permanently so the losses are irreversible.
- Message corruption: modification of content by attacker.
- False node: Insertion of malicious node is most dangerous attacks; as malicious code could spread to all the nodes.

Various Security Mechanisms:

- Low-Level Mechanism: for securing sensor network:
  - Key establishment
  - Secrecy and authentication
  - Privacy
  - Robustness
  - Secure routing
- Key establishment and trust setup: Establishment of cryptographic keys is the primary requirement.
- Secrecy and authentication: requires protection against eavesdropping, modification of packets.
- Privacy
- Robustness to communication denial of service
- Secure routing

Thus network security is an important field due to rapid growth in use of internet. To improve on security more powerful security mechanism is required.

Archana Ingle

Fast-Track Your IOT, WSN HEALTHCARE

The use of IoT technology is rapidly increasing in healthcare development and smart healthcare system for fitness programs, monitoring, data analysis, etc. To improve the efficiency of monitoring, various studies have been conducted in this field to achieve improved precision.

The COVID-19 pandemic and other ongoing health crises have underscored the need for prompt healthcare services worldwide. The traditional healthcare system, centred around hospitals and clinics, has proven inadequate in the face of such challenges. Intelligent wearable devices, a key part of modern healthcare, leverage Internet of Things technology to collect extensive data related to the environment as well as psychological, behavioural, and physical health. However, managing the substantial data generated by these wearables and other IoT devices in healthcare poses a significant challenge, potentially impeding decision-making processes.

IoT healthcare applications

IoT is the growing technology in the internet environment in conjunction with real time connected objects. It is popular in many different industries because of convergence from the simple object into a smart object. This has a long term impact on the health monitoring, administration and clinical service to patient’s physiological information. Patients are connected with sensors and the data has been associated with control devices, then it forwards to the health-monitoring unit. Sometimes data are stored in the cloud, which helps to manage the number of data with security. An important area in the IoT is security because when dealing with data transmission from the sensor to cloud center it is a possible loss of integrity and confidentiality and also it is complex to encrypt the data received from low resource devices. Cloud is a distributed environment so that it is the best option to store the medical data which more flexible for remotely caring patients accessed by doctors and Vice Versa. The IoT and cloud start handshake for realtime processing which turns to give complexity in architecture to sending and receiving data. To reduces the complexity in IoT and cloud a novel framework is proposed to manage the IoT realtime data and scientific-based unrelated IoT data then tested the cloud environment provides Software as a Service (SaaS) in the hybrid cloud environment.

Everywhere IOT is used in healthcare. But some examples I mention here so that generalised idea we will get.

Remote patient monitoring

Glucose monitoring

Heart rate monitoring

Hand hygiene monitoring

Depression and mood monitoring

Ingestible sensors

Trackable inhalers

IOT based ambulance

Smart wheelchair

Big data in IoT healthcare

In recent years, Big data storage technology is essential to store huge volumes of clinical data. The cloud storage becomes huge its manage by the technology called Big data. The recent studies say the combination of Big data and cloud influencing remote healthcare. Amazon Elastic MapReduce (EMR) provides a different method to handle the big data and get onto the cluster. The Amazon EMR has a different function to load the data into Hbase cluster. Loading the sensor data from Amazon S3 to Hbase by using the tool as an Apace pig. Apace pig is used for analyzing the data in the distributed database hence healthcare application can dramatically extend the scalable feature

Security in IoT

Security has been the major concern in the IoT because the hackers or the attacker can easily access the sensor data, so it is important to analyze the recent security methods in IoT. The IoT-oriented data placement method with privacy preservation named IDP is developed. In this proposed method main aim is to optimize the data access time, increase resource utilization and reduce energy consumption by satisfying the constraints of data privacy. The privacy-preserving and energy saving is achieved using the algorithm called Non-Dominated Sorting Genetic Algorithm II (NSGA-II).

Challenges in healthcare IoT

IoT has been adopted in the different types of applications and provide different support for the healthcare system such as patient monitoring, a smart home system for the diabetic patient. Major problems occur in the healthcare system are listed as follows.

IoT paves the way for high flexibility, i.e., the patient requires constant care and he/she can live in the home instead of the hospital and be monitored regularly using IoT technology. Some wearable devices like sensors make uncomfortable for the patient’s body.

The data transmitted from the sensor to the control device and further transmitted to the monitoring center, which will affect the quality of the data due to noise. Better architecture helps to transmit the data without affecting its nature. Noise removal technique can also help to enhance the data signal.

Most of the existing method in ECG monitoring involves analyzing the signal in a supervised manner. This increases the cost and it may produce the error in detection. Machine learning can be applied in analyzing the signal, which helps to improve efficiency and reduce expenses.

An increasing number of sensors and the devices require higher energy to process, and it increases the power leakage and energy consumption. An optimization algorithm can be used to reduce the usage of energy.

Monitoring many numbers of users in the IoT requires more storage and mainframe, which can be overcome by storing the data in the Cloud. However, the IoT integrated with the cloud increases the complexity.

Another important problem in the IoT is privacy as the devices are more vulnerable to the attack. These devices are low resource constraints and are difficult to apply encryption techniques on them.

Pratik Parsewar

What is mixed reality?

Mixed reality is the next wave in computing following mainframes, PCs, and smartphones. Mixed reality is going mainstream for consumers and businesses. It liberates us from screen-bound experiences by offering instinctual interactions with data in our living spaces and with our friends. Online explorers, in hundreds of millions around the world, have experienced mixed reality through their handheld devices. Mobile AR offers the most mainstream mixed reality solutions today on social media. People may not even realize that the AR filters they use on Instagram are mixed reality experiences. Windows Mixed Reality takes all these user experiences to the next level with stunning holographic representations of people, high fidelity holographic 3D models, and the real world around them.

Mixed reality is a blend of physical and digital worlds, unlocking natural and intuitive 3D human, computer, and environmental interactions. This new reality is based on advancements in computer vision, graphical processing, display technologies, input systems, and cloud computing. The term "mixed reality" was introduced in a 1994 paper by Paul Milgram and Fumio Kishino, "A Taxonomy of Mixed Reality Visual Displays." Their paper explored the concept of a virtuality continuum and the taxonomy of visual displays. Since then, the application of mixed reality has gone beyond displays to include:

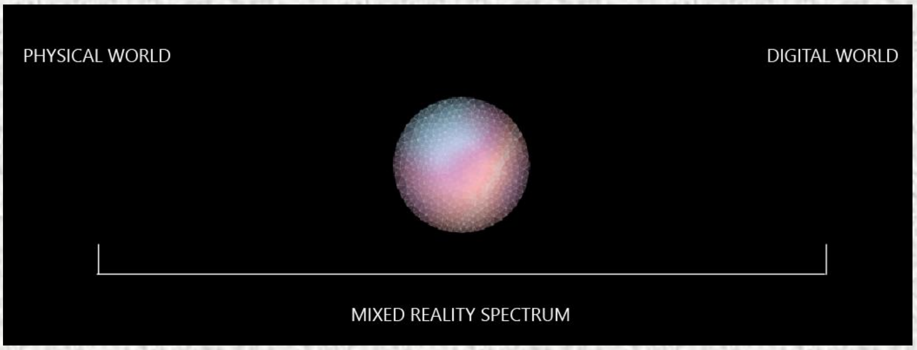
Environmental understanding: spatial mapping and anchors.

Human understanding: hand-tracking, eye-tracking, and speech input.

Spatial sound.

Locations and positioning in both physical and virtual spaces.

Collaboration on 3D assets in mixed reality spaces.



Environmental input and perception

In recent decades, the relationship between humans and computers has continued to evolve by means of input methods. A new discipline has emerged that's known as human-computer interaction or "HCI". Human input can now include keyboards, mice, touch, ink, voice, and Kinect skeletal tracking.

Advancements in sensors and processing power are creating new computer perceptions of environments based on advanced input methods. This is why API names in Windows that reveal environmental information are called the perception APIs. Environmental inputs can capture:

a person's body position in the physical world (head tracking)

objects, surfaces, and boundaries (spatial mapping and scene understanding)

ambient lighting and sound

object recognition

physical locations

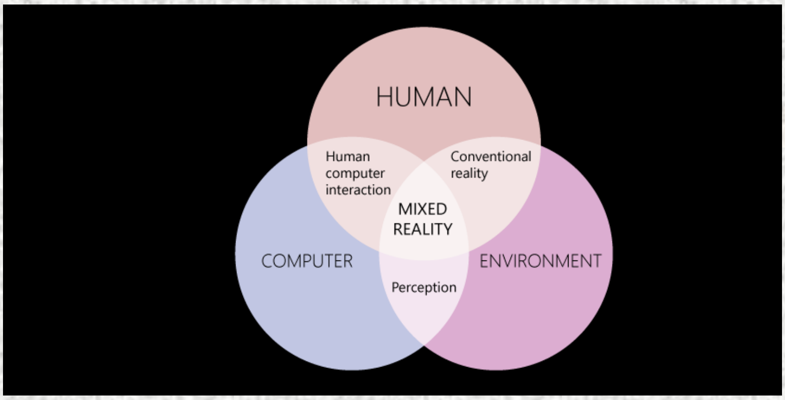


Image: The interactions between computers, humans, and environments.

A combination of three essential elements sets the stage for creating true mixed reality experiences:

Computer processing powered by the cloud

Advanced input methods

Environmental perceptions

As we move through the physical world, our movements are mapped in a digital reality. Physical boundaries influence mixed reality experiences such as games or task-based guidance in a manufacturing facility. With environmental input and perceptions, experiences start to blend between physical and digital realities.

Kushal Suvarna

The Future Scope of Electronics & Communications Engineering in India

The field of Electronics and Communications Engineering (ECE) is at the cusp of a new era in India, driven by rapid technological advancements, digital transformation, and the increasing integration of electronics in everyday life. ECE encompasses the study, design, and application of electronic devices, circuits, and communication equipment. As India strides towards becoming a global technology hub, the scope for ECE professionals is expanding exponentially. This article explores the future landscape of ECE in India, focusing on emerging trends, opportunities, and challenges.

Emerging Trends in ECE

1. **Internet of Things (IoT)**

The IoT revolution is making devices smarter and more interconnected. In India, the adoption of IoT technologies is expected to accelerate in sectors like agriculture, healthcare, smart cities, and manufacturing, opening vast avenues for ECE professionals.

2. **5G and Beyond**

With India gearing up for the rollout of 5G services, the demand for ECE engineers skilled in next-generation telecommunication technologies is on the rise. The leap to 5G and eventually to 6G will necessitate innovations in network infrastructure, requiring expertise in areas such as millimetre-wave technology, network slicing, and edge computing.

3. **Artificial Intelligence and Machine Learning (AI & ML)**

AI and ML are becoming integral to electronic devices and communication systems, enhancing their capabilities and efficiency. ECE engineers are pivotal in integrating AI and ML algorithms with electronic hardware, pushing the boundaries of what devices can achieve.

4. **Renewable Energy Systems**

As India moves towards sustainable energy solutions, there is a growing need for ECE professionals skilled in designing and managing renewable energy systems, including solar photovoltaic (PV) technology, wind energy systems, and energy storage technologies.

5. **Semiconductor Fabrication and Design**

With initiatives like the Semiconductor Mission, India is focusing on developing its semiconductor fabrication capabilities. This push towards semiconductor self-reliance opens up opportunities for ECE engineers in VLSI design, semiconductor materials science, and nanotechnology.

Opportunities for ECE Engineers in India

1. **Research and Development (R&D)**

R&D in electronics and communication technologies is thriving, with opportunities in both public and private sectors. ECE professionals can engage in cutting-edge research in areas like nano electronics, wireless communication, and embedded systems.

2. **Defence and Aerospace**

India's focus on strengthening its defence and aerospace sectors spells significant opportunities for ECE engineers. From radar and communication systems to electronic warfare and satellite technology, the scope for contribution is vast.

3. **Telecommunications**

With the ongoing expansion of telecom infrastructure and services across India, ECE professionals have a critical role in designing, implementing, and maintaining telecommunication networks.

4. **Consumer Electronics**

The consumer electronics market in India is booming, driven by increasing consumer demand for smart gadgets. ECE engineers are essential in the design, development, and testing of these products.

Challenges and the Way Forward

Despite the bright prospects, there are challenges that need addressing to harness the full potential of ECE in India:
Skill Gap: Bridging the gap between academic curricula and industry needs is crucial. Emphasis on practical skills, internships, and industry collaborations can enhance employability.
Research Infrastructure: Strengthening the research infrastructure and fostering a culture of innovation will be key to maintaining competitiveness in the global arena.

Policy Support: Government policies play a pivotal role in shaping the future of ECE in India. Initiatives to support start-ups, R&D, and manufacturing in electronics can drive growth.

Conclusion

The future scope of Electronics and Communications Engineering in India is vibrant and promising, fuelled by technological innovations and government initiatives. As the country makes strides in areas like IoT, 5G, AI, and renewable energy, the demand for skilled ECE professionals is set to soar. By addressing existing challenges and capitalizing on emerging opportunities, India can cement its position as a global leader in electronics and communication technology.

Meena Perla

Fingerprint Combination using Super Template for Privacy Protection

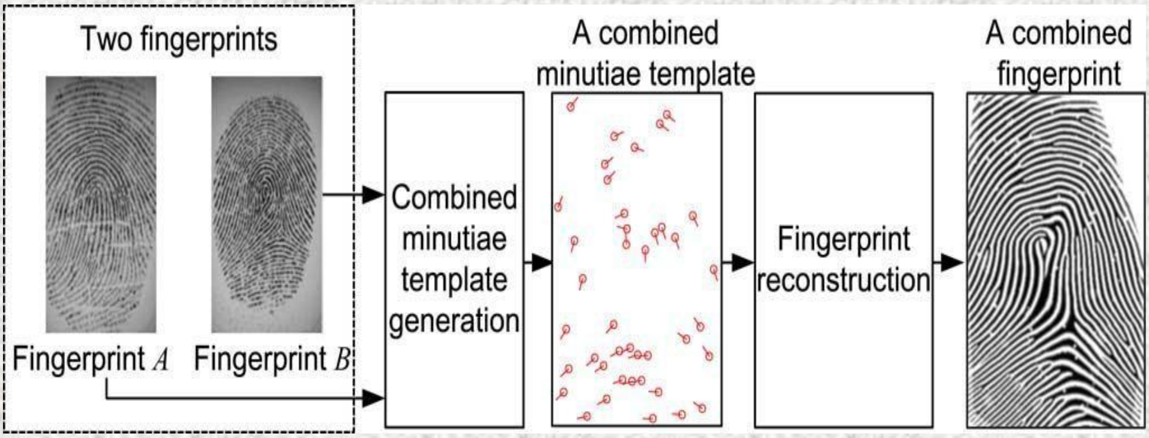
Fingerprint is defined as an impression of the markings of the inner surface of the finger. This concept has been existence for thousands of the year. Fingerprints were also used in the 19th century by the policemen for identification of regular criminals. Though the fingerprint biometrics first used in the 1970s as an automated technology.

The commercial applications started using fingerprint biometrics for controlling physical access to buildings, offices etc. Then the using advance technology, this trend continues grow. The increasing need to reduce instances of fraud as well as to provide secured access.

Identification systems depends on three key elements: 1) biographical identifiers (e.g., address, profession, education, and marital status), 2) biometric identifiers (e.g., fingerprint, iris, voice, and gait and 3) attribute identifiers (e.g., Social Security Number, driver's license number, and account number. It is easy for a human being to misrepresent attribute and biographical identifiers; however, biometric identifiers depend on intrinsic physiological characteristics that are difficult to misrepresent or change.

The primary reason of using a biometric system is to provide non reputable authentication. Authentication implies that (i) only genuine or official users are able to access the physical or logical resources protected by the biometric system and (ii) impostors are prevented from accessing the protected resources. While a biometric system can be compromised in a number of ways, one of the potentially damaging attacks is the leakage of biometric template information. The leakage of this template information to unauthorized individuals constitutes a serious security and privacy threat. Therefore, the propose work a model of creating a combined minutiae template. By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.

COMBINED FINGERPRINT GENERATION


Two fingerprints
Fingerprint A
Fingerprint B
Combined minutiae template generation
A combined minutiae template
Fingerprint reconstruction
A combined fingerprint

In a combined minutiae template, the minutiae positions and directions are extracted from two different fingerprints separately. These minutiae positions and directions share a similar topology to those from an original fingerprint. Therefore, the combined minutiae template has a similar topology to an original minutiae template. Some existing works have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image. Fig. 5.8 shows our process to generate a combined fingerprint for two different fingerprints. Given any two different fingerprints as input, we first generate a combined minutiae template using our combined minutiae template generation algorithm.

Then, a combined fingerprint is reconstructed from the combined minutiae template using one of the existing fingerprint reconstruction approaches.

We will not be able to match the corresponding combined fingerprint by using a general fingerprint matching algorithm. While the purpose of generating a combined fingerprint is to issue a new virtual identity for two different fingerprints, which should be matched using general fingerprint matching algorithms.

Among the existing fingerprint reconstruction approaches, our previous work achieves excellent performance. We here adopt this approach for generating a combined fingerprint from a combined minutiae template. However, the work in does not incorporate a noising and rendering step to make the reconstructed fingerprint image real- look alike. To create a real-look alike fingerprint image from a set of minutiae points, we further apply a noising and rendering step after adopting the work in, which are illustrated in results.

Bharat Warude

Use of deep convolutional network for image tampering detection

Due to availability of many advanced image editing software, spreading of fake images on social media is one of the major concern.

- Spread of fake images on social media can reap controversies. Hence the need for an image forensic tool to help people determine whether the image spread is real or fake.
- The content security of an image become a crucial issue for scientists and engineers.
- Recently, some deep convolutional neural networks methods have been applied in the image classification, image forensic etc. which have shown better performance than the traditional active and passive methods of image forgery detection.
- The proposed system presents a new image forgery detection method based on deep learning technique, which utilizes a convolutional neural network (CNN) to automatically learn from the input RGB colour images.
- The proposed method also uses ELA (Error Level Analysis) and CNN algorithm where ELA find out the compression ratio between original image and fake image as the original image compression and fake image compression is different.
- Experimental results show that the proposed CNN is specifically designed for image splicing and copy-move type of image forgery detection application.

Image Forgery Techniques:

Image forgery is the manipulation or alteration of an image.

- **Active Approach**

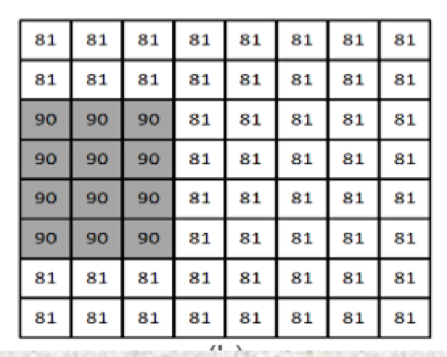
A. Digital watermarking
B. Digital signature

- **Passive Approach**

A. Image splicing:
B. Copy-move forgery:
C. Image Retouching:

Error Level Analysis (ELA) for Image Forgery Detection:

Error level analysis is one technique for knowing images that have been manipulated by storing images at a certain quality level and then calculating the difference from the compression level. Error level analysis is one technique for knowing images that have been manipulated by storing images at a certain quality level and then calculating the difference from the compression level. When JPEG was first saved, then it will compress the image the first time, most editing software like adobe photoshop, gimp, and adobe light room support JPEG compressing operation. If the image is rescheduled using image editing software, then compressed again. So it shows that the original image when the first image is taken using a digital camera has been compressed twice, first use the camera and the second is editing software. When viewed with the naked eye the image looks the same, but by using this method it will look the difference between a forgery image with the original image. Original images from digital cameras should have high ELA values. When the image is resaved, using ordinary human vision does not show a significant degree of difference, but ELA shows the dominant black and dark colors. If this image is resaved again it will decrease the image quality. If the original image is then modified, ELA will show the modified area has a color with a higher ELA level.



81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81

Fig.1.Error Level Analysis on image

Deep learning models for image forgery detection:

In recent years, machine learning and neural networks, such as convolutional neural networks(CNNs), have shown to be capable of extracting complex statistical features and to efficiently learn their representations, allowing to generalize well across a wide variety of computer vision tasks, including image recognition and classification and so on. The extensive use of such networks in many areas has motivated and led the multimedia forensics community to comprehend if such technological solutions can be employed to exploit source identification.

One approach to image forgery detection using deep learning is to train a convolutional neural network (CNN) on a dataset of both genuine and forged images. The CNN can then be used to classify new images as either genuine or forged based on the features it has learned to recognize A deep learning-based approach to image forgery detection, specifically using Error Level Analysis (ELA) with Convolutional Neural Networks (CNNs) and a pre-trained model. The study compares the performance of the two models and provides an in-depth analysis of the results. A primary method in image forgery detection is the Error Level Analysis (ELA), a technique that quantifies the compression levels across an image Error Level Analysis (ELA), a passive method for finding fake images, assesses how consistently different levels of compression are used throughout an image. The compression levels of the edited area in an image are frequently different from the surrounding portions. ELA draws attention to these discrepancies, which makes it simpler to spot forgeries.

Graphical User Interface (GUI) of Image Tampering Detection

The homepage of the Image Tampering Detection project, featuring an introduction to the project with a focus on its objectives. The "About our project" section succinctly outlines key details. Three prominent deep learning models, namely VGG19, EfficientNet-B2, and the ELA CNN (Best Model), are highlighted in concise bullet points.

The interface unveils a user-friendly design featuring a "Select Image File" option, allowing users to choose an image file easily. Following the selection, a designated button triggers the prediction process for image tampering.

AN outcome of the tampering detection process, reveals that the chosen image has indeed undergone manipulation. The interface effectively communicates the detection results, signaling to the user that tampering has been identified.

Sonali Gaikwad

Agriculture 4.0- Technology driven Agriculture Revolution

In the era of Industry 4.0, agriculture is undergoing a transformational shift, leveraging cutting-edge technologies to address the challenges of feeding a growing global population while minimizing environmental impact. This article explores the concept of Agriculture 4.0 and its implications for the future of farming. From precision agriculture and smart farming techniques to the utilization of drones, sensors, and machine learning algorithms, Agriculture 4.0 promises to revolutionize every aspect of the agricultural value chain. By harnessing the power of data-driven decision-making and automation, farmers can optimize resource usage, improve crop yields, and mitigate risks associated with climate change and fluctuating market demands. However, realizing the full potential of Agriculture 4.0 requires overcoming barriers such as cost constraints, digital literacy, and privacy concerns. Through collaboration between farmers, technology developers, and policymakers, Agriculture 4.0 has the potential to drive sustainable agricultural development and ensure food security for generations to come.

Fig 1: Agriculture 4.0

"Agriculture 4.0" typically refers to the integration of advanced technologies such as automation, robotics, artificial intelligence, and big data analytics into the agricultural industry to enhance efficiency, productivity, and sustainability. It marks the digitalization of food and agriculture systems using AI, IoT, automation and other technologies to create a hyper-connected network of farms, machines and factories.

Some of the key game changers of Agriculture 4.0 are:

- Adoption of technology to enhance quality of produce:

Urban Farming	Adoption of aeroponic technology for indoor vertical farming
Genetic Farming	Adoption of Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) for genome editing to create enhanced breeds with higher yields and resilience in adverse conditions

3D printing	Creating food objects using printers with hydrocolloids to replace base ingredient of food with other renewables like algae or grass

- Adoption of cross-industry horizontal solutions

IoT	Using IoT for effective surveillance of farms with the help of sensors (light, humidity, temperature, soil moisture, health of equipment), automating irrigation systems, etc.
Drones	Utilizing drones for soil health scans, monitoring crop health, spraying fertilizers, forecasting crop yield and tracking weather conditions
Precision Farming	Big Data Analytics and Robotics-enabled approach that monitors farms and collects information like weather, yield, NDVI, crop moisture, terrain type, soil map from different sources to manage and optimize crop yield
Data Analytics	Making data driven decisions by analyzing data collected from IoT sensors at farms and the equipment used to deliver optimized smart farming
Nanotechnology	Application of novel nano tools like nanofertilizers, nanopesticides, nanobiosensors and nano-enabled remediation strategies for contaminated soils, focused on improving yields and food quality
Telematics	Machine to machine communication between hardware and sensors to automate decisions in farming. Application – precision-sowing that links seed spreader to soil sensors and leads to effective sowing as per soil conditions
Artificial Intelligence and Machine Learning	Application of autonomous robots to handle manual tasks, leveraging computer vision and deep learning algorithms for crop and soil monitoring, applying predictive analytics to track and predict environmental impact on crop yield
Big Data	Data mining large data sets generated by adoption of ICT in farming to provide actionable farming solutions that ensure profitability, efficiency and sustainability.

	Big data-enabled predictive modelling increasingly being used in crop insurance.
Blockchain	Enhancing agricultural supply chains by creating a shared, decentralized blockchain ledger of agricultural information that serves as a transparent and trusted source of truth. Empowers farmers and creates a direct link between farmers and consumers with traceability options

Nonetheless, there is still a great deal of reticence towards this new way of understanding agriculture and the new technologies associated with it. However, there is no doubt that agriculture 4.0 offers a number of advantages.

1. Increased Efficiency: Agriculture 4.0 technologies such as precision agriculture, automation, and robotics enable farmers to optimize resource usage, including water, fertilizers, and pesticides. By precisely targeting inputs based on real-time data and analytics, farmers can minimize waste and improve overall efficiency.
2. Enhanced Productivity: Advanced technologies like AI-driven predictive analytics and machine learning algorithms empower farmers to make data-driven decisions regarding crop management, irrigation scheduling, and pest control. This leads to higher crop yields and improved farm productivity.
3. Cost Savings: By optimizing resource utilization, reducing input wastage, and streamlining farm operations through automation, Agriculture 4.0 helps farmers cut down on production costs. Additionally, predictive maintenance of machinery and equipment reduces downtime and maintenance expenses.
4. Sustainability: Sustainable farming practices are promoted through Agriculture 4.0 by minimizing environmental impact, conserving natural resources, and reducing greenhouse gas emissions. Precision farming techniques help mitigate soil degradation, water pollution, and deforestation, contributing to long-term environmental sustainability.
5. Risk Mitigation: Agriculture 4.0 enables farmers to better manage risks associated with weather variability, pests, diseases, and market fluctuations. Real-time monitoring and early warning systems help farmers anticipate and respond to potential threats, thereby minimizing crop losses and financial risks.
6. Data-Driven Decision-Making: Access to comprehensive data and analytics allows farmers to gain valuable insights into their operations, crop performance, and market trends. This enables informed decision-making regarding planting, harvesting, marketing, and investment strategies, leading to better outcomes and profitability.
7. Improved Quality and Traceability: With the use of sensors, IoT devices, and blockchain technology, Agriculture 4.0 facilitates improved traceability and quality control throughout the supply chain. Farmers can track the entire production process, from seed to shelf, ensuring product quality, safety, and authenticity, which is increasingly important to consumers and regulatory bodies.
8. Global Food Security: By increasing agricultural productivity, optimizing resource use, and reducing post-harvest losses, Agriculture 4.0 contributes to global food security. The ability to produce more food sustainably is crucial for feeding a growing global population, particularly in the face of climate change and dwindling arable land.

These advantages highlight the transformative potential of Agriculture 4.0 in addressing the evolving needs and challenges of the agricultural sector while promoting sustainable and resilient farming practices.

Nutan Malekar

COGNITIVE RADIO

INTRODUCTION:

Cognitive radio (CR) is a form of wireless communication in which a transceiver can *intelligently detect which communication channels are in use and which ones are not.* The transceiver then instantly moves into vacant channels, while avoiding occupied ones. These capabilities help optimize the use of the available radio frequency (RF) spectrum**.**

WHY COGNITIVE RADIO?

The wireless RF spectrum is a limited resource, usually allocated through a licensing process. In the U.S., it is the joint responsibility of the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The FCC administers the spectrum for non-federal (e.g., commercial) use, while the NTIA does the same for federal (e.g., military, FBI) use. The allocated (licensed) spectrum is not always used optimally. As a result, some bands are overcrowded (e.g. GSM cellular networks), while others are relatively unused (e.g., military). This spectrum inefficiency limits the amount of data that can be transmitted to users and lowers service quality. As the number of connected devices in use continues to grow, this limited resource is fast becoming a *scarce* resource. Cognitive radio is an efficient way to use and share this resource intelligently, optimally and fairly. It also minimizes interference to other users. And, by avoiding occupied channels, it increases Spectrum Efficiency and improves the quality of service (QoS) for users.

COGNITIVE RADIO TECHNIQUES:

The 2 different types of Cognitive Radio are:

- Spectrum Sensing
- Spectrum Database

Spectrum Sensing is further subdivided into :

- Non Co-operative: It Acts on its own and decisions are based upon signal detection and pre-loaded information. Examples of Non-Cooperative Spectrum Sensing algorithms are: Energy Detection, Cyclo stationary, Match Filter and Waveform Based algorithms.
- Co-operative: In this kind of sensing, CR device shares spectrum sensing information among themselves and the Decisions are taken by a control unit or a mesh kind of network.

COGNITIVE RADIO ARCHITECTURE:

With the development of CR technologies, secondary users who are not authorized with spectrum usage rights can utilize the temporally unused licensed frequency bands owned by the primary users.

Secondary Network: A Secondary Network refers to a network composed of a set of secondary users with/without a secondary Base Station. Secondary users can only access the licensed spectrum when it is not occupied by a primary user.
The opportunistic spectrum access of secondary users is usually coordinated by a secondary Base Station, which is a fixed infrastructure component serving as a hub of the secondary network. Both secondary users and secondary Base Stations are equipped with CR functions. If several secondary networks share one common spectrum band, their spectrum usage may be coordinated by a central

network entity, called spectrum broker. The spectrum broker collects operation information from each secondary network, and allocates the network resources to achieve efficient and fair spectrum sharing.

Primary Network: A Primary Network is composed of a set of primary users and one or more primary Base Stations. Primary users are authorized to use certain licensed spectrum bands under the coordination of primary Base Stations. Their transmission should not be interfered by secondary networks. Primary users and primary Base Stations are in general not equipped with CR functions. Therefore if a secondary network share a licensed spectrum band with a primary network, besides detecting the spectrum white space and utilizing the best spectrum band, the secondary network is required to immediately detect the presence of a primary user and direct the secondary transmission to another available band so as to avoid interfering with primary transmission.

COGNITIVE TRANSCEIVER ARCHITECTURE:

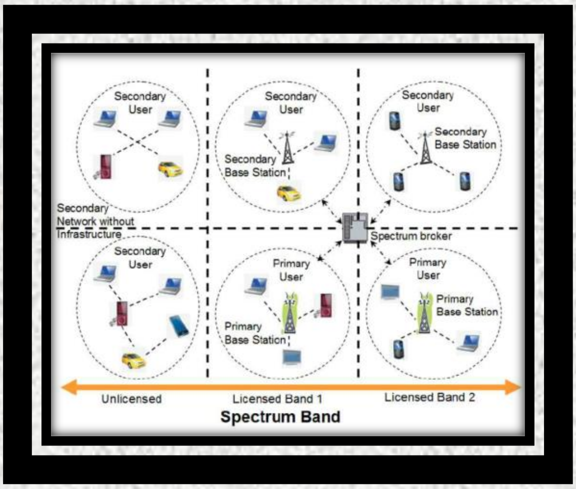


Fig: Cognitive Radio Architecture

The basic structure of a cognitive transceiver consists of three parts: Radio Frequency (RF), Analog to Digital Converter (ADC), and baseband processing. Depending on the particular type of cognitive radio, one or more of those components is made adaptive. In a spectrum-sensing cognitive radio, only the RF front end is adaptive and different from a conventional RX. For a fully cognitive radio, the baseband processing also has to be adaptive. This can be most easily achieved by implementing the baseband processing as software on a Digital Signal Processor (DSP).

BENEFITS OF COGNITIVE RADIO:

The Benefits of a Cognitive Radio are:

- It offers better spectrum utilization and efficiency.
- It improves link reliability.
- It is lower in cost.
- It uses advanced network topologies.
- It has simple network architecture.
- It is easy in configuration and easy to upgrade.
- It is less in complexity.

DRAWBACKS OF COGNITIVE RADIO:

The Drawbacks of a Cognitive Radio are:

- There is no complete automation and it requires user intervention for any changes to be implemented.
- It always requires multi band antenna.
- Security concern: There are more chances open for attackers in cognitive radio technology compare to traditional wireless networks. The data may be eavesdropped or altered without notice. The channel might be jammed or overused by the adversaries.
- QoS (Quality of Service) in Cognitive radio is affected due to its adverse effects.

Translation of observations into actions is a big challenge in cognitive radio.

APPLICATIONS OF A COGNITIVE RADIO:

The Applications of a Cognitive Radio are:

- As, the capacity of military communications is limited by radio spectrum scarcity. It is due to static frequency assignments in many unused applications, where a large amount of spectrum is idle. Using CR concept bandwidth crunch problem can be solved by allocating bandwidth as per need and application. Therefore, CR can provide military an adaptive, seamless, and secure communications.
- A CR network can also be used to provide public safety and security. A natural disaster or terrorist attack can destroy existing communication infrastructure. To provide search and rescue operations, an emergency network is required. CR networks can play an important role to provide communication as they have capability to detect unused spectrum and reconfigure itself to provide service without delay. Thus it provides public safety and security with dynamic spectrum selection.
- CR networks can also provide commercial markets for existing wireless technologies. Since CR can intelligently determine which communication channels are available and which are in use, can automatically switches to an unused or unoccupied channel. Thus provides additional bandwidth for rapidly growing data applications. Also this adaptive channel allocation avoids the need of expensive redeployment.

CONCLUSION:

In Conclusion, Cognitive Radio is a smart technology that makes wireless communication better by using available frequencies more efficiently. It helps reduce problems like network congestion and interference while making sure we can use our wireless devices more effectively. As our demand for wireless services keeps growing, Cognitive Radio is like a helpful tool that ensures we can stay connected without running out of space in the airwaves. It's a vital part of the future of wireless communication.

Sayanna Mukharjee (BE)

Network Management Function and Configuration Management

The primary purpose of network management is to deliver a secure, reliable, and high-performing network to end-users, including business users in the enterprise and end customers. Network management was always a crucial part of the IT task list, and it has become even more critical in the wake of COVID-19. Distributed companies primarily rely on network management to keep different enterprise functions and teams connected. Network management is also responsible for managing data flow in and out of different host environments such as on-premise servers, private clouds, and public cloud platforms.
Different network management functions
Perfomance management
Fault management
Configuration management
Security management
Accounting management

1. Performance management
-As the name indicates, performance management functions are related to improving the performance of network system.
-It is used to monitor the performance parameters of all connections used in optical network.
- These functions are also used to take certain actions of the network parameters, according to the requirements.

2. Fault management
- The fault management functions are related to search for the failure in network and then to generate indication of failure
- For example, if the incoming light power from source is below the threshold level then these function generates, the corresponding alarm
-Similarly, if there is a failure in any component of optical network then fault management functions give indication of this failure and then the particular component is isolated
-During such failures; the optical traffic is routed through another path

3. Configuration Management
- These functions are related to managing of equipment’s used in optical network, managing various optical connection in the network and managing adaption of client signal
- These functions are used to remove or add network equipment in the network
- For making new connections in the network or removing some connections; again these functions are used
- When external client enters any signal then to convert it into the signal which is compatible for optical network; adaption configuration management functions are used

4. Security management
- As the name indicates; security management functions are related to the security of optical network system

- These functions are related to authentication of user and giving access permission to authenticated users
- These functions are also related to giving protection to the data, so that unauthorised user should not attack the data
- For the data protection, encryption process is used at the transmitter and description process is used at the receiver

5. Accounting management
- These management functions are related to billing information
- Using these function the history of network components is recorded
Configured Management
-A configuration management function has three parts: -
1. Equipment Management
2. Connection management
3. Adaptation management

1. Equipment Management
- In general, the principles of managing optical networking equipment are no different from those of managing other high speed networking equipment
- It must be able to keep track of the actual equipment in the system as well as the equipment in each network element and its capabilities
- For example, in a terminal of a point to Point WDM system, we may want to keep track of the maximum number of wavelengths and the number of wavelengths currently equipped, whether or not there are optical pre and power amplifiers and so forth

2. Connection management
- In optical networks provides light paths, circuit switched connection to its user.
- Connection management deals with setting up connections, keeping track of them, and taking them down when they are not needed anymore.
- The process usually involves configuring. Equipment from a variety of vendors each with its own management system, and usually one network element at a time.
- Service providers in many cases deploy equipment only when needed.

3. Adaptation management
- Adaptation management is the function of taking the client signals and covering them to a form that can be used inside the optical layer. This function includes the following:
i. Covering the signal to the appropriate wavelength, optical power level, and other optical parameters associated with the optical layer. The WDM is received and converted into standardized signal, such as a short-reach SONET signal.
ii. Adding and removing appropriate overheads to enable signal to be managed inside the optical layer.

- Aasavaree Rane(BE)

Understanding and Mitigating Peak-to-Average Power Ratio (PAPR) in OFDM Systems

Introduction

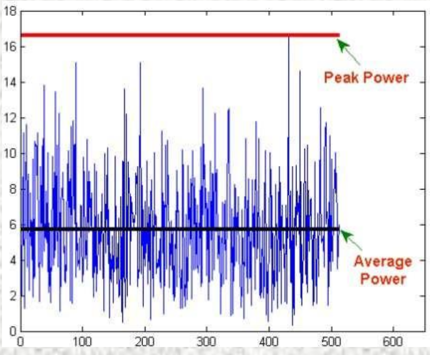
Orthogonal Frequency Division Multiplexing (OFDM) has become the cornerstone of many wireless communication systems, including Wi-Fi, LTE, and 5G. Despite its numerous advantages, OFDM suffers from a significant drawback known as the Peak-to-Average Power Ratio (PAPR). PAPR refers to the ratio of the maximum instantaneous power to the average power of the OFDM signal. In this article, we will examine the causes of high PAPR in OFDM systems and delve into various techniques used to mitigate its impact.

Causes of High PAPR in OFDM

Several factors contribute to the high PAPR in OFDM signals. These include the nature of the OFDM signal itself, the presence of subcarriers, and the inherent characteristics of the modulation scheme. This section provides an in-depth analysis of these factors and their impact on PAPR.

Effects of High PAPR

Understanding the consequences of high PAPR is crucial for designing robust communication systems. Non-linear distortions in power amplifiers, reduced power efficiency, and increased bit error rates are among the detrimental effects of elevated PAPR. This section explores the practical implications of high PAPR on system performance.

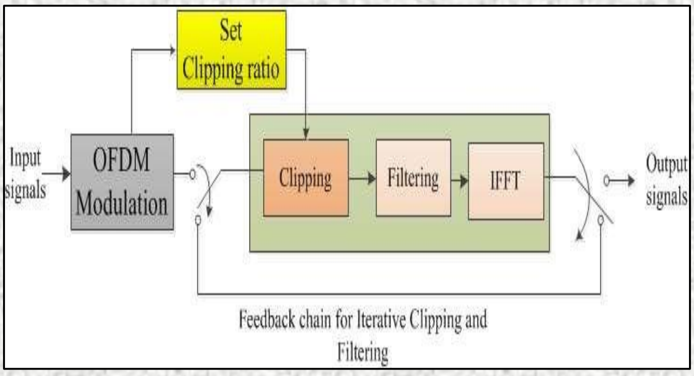


Mitigation Techniques

To overcome the challenges posed by high PAPR, researchers and engineers have developed various mitigation techniques. This section provides a comprehensive overview of these techniques, including.

Clipping and Filtering

The simplest method involves clipping the peaks of the OFDM signal and subsequently filtering out the introduced distortion. This technique is easy to implement but may lead to out-of-band interference.

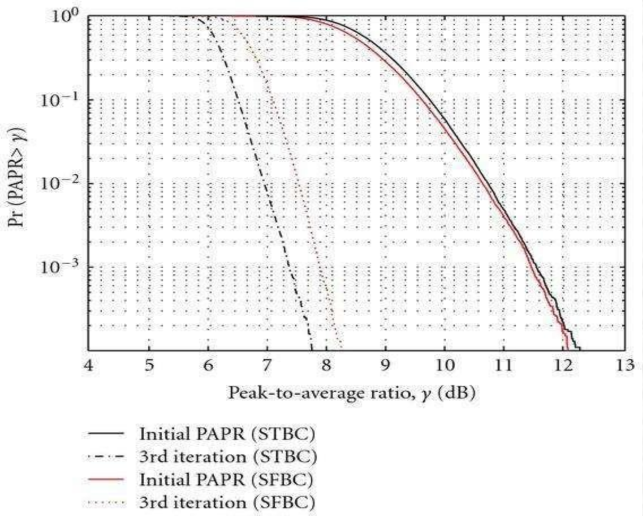


Techniques

Coding schemes such as selected mapping (SLM) and partial transmit sequence (PTS) introduce redundancy to the signal, reducing the probability of high peaks.

Active Constellation Extension

By modifying the signal constellation during transmission, active constellation extension aims to minimize the probability of high peaks.



Tone Reservation

In this technique, specific subcarriers are reserved to reduce the overall PAPR of the signal. Tone reservation requires careful subcarrier selection and allocation.

Peak Windowing

By applying windowing functions to the OFDM signal, peak values can be effectively reduced. However, this method may introduce additional complexity.

Performance Evaluation

This section presents a comparative analysis of the aforementioned PAPR mitigation techniques. Through simulations and real- world experiments, we assess the effectiveness of each method in terms of PAPR reduction, computational complexity, and impact on system performance.

Conclusion

In conclusion, understanding and addressing the challenges posed by high PAPR in OFDM systems are crucial for achieving reliable and efficient communication. As the demand for higher data rates and spectral efficiency continues to grow, researchers and engineers must continue to explore innovative techniques to mitigate PAPR and enhance the performance of OFDM-based communication systems.

MAYUR PATIL(BE)

Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are pivotal in the realm of data monitoring and collection. These networks consist of self-configuring nodes, small in size, which communicate via radio signals. Deployed in large numbers, they sense, monitor, and comprehend the physical environment. Given the limitations of individual nodes, collaboration through wireless communication is essential, enabling efficient task completion and comprehensive data gathering across various domains.

INTRODUCTION

Wireless Sensor Networks (WSNs) are pivotal in the realm of data monitoring and collection. These networks consist of self-configuring nodes, small in size, which communicate via radio signals. Deployed in large numbers, they sense, monitor, and comprehend the physical environment. Given the limitations of individual nodes, collaboration through wireless communication is essential, enabling efficient task completion and comprehensive data gathering across various domains.

CHALLENGES IN WSN’s

WSNs face challenges such as limited energy resources, interferences, and node failures, which significantly impact network operations. Efficient energy management, interference mitigation, and fault tolerance mechanisms are crucial to enhancing network performance and ensuring seamless operation.

DESIGN CONSIDERATION

Effective WSN design requires careful consideration of factors like multi-hop wireless communication, energy-efficient operation, auto-configuration capabilities, collaboration and in-network processing, and a data-centric approach. These elements ensure the WSN meets the demands of diverse applications.

WSN ARCHITECTURE

WSNs can have a layered architecture with nodes communicating directly with a central base station, or a clustered architecture where nodes self-organize into groups with cluster heads coordinating communication. These approaches offer different trade-offs in scalability and energy efficiency.

CONCLUSION

WSNs serve as versatile tools across various applications, from disaster relief to precision agriculture, healthcare, and supply chain management. By gathering real-time data, optimizing processes, and enhancing efficiency, WSNs enable industries and communities to achieve greater resilience, productivity, and sustainability. As technology advances, the potential for WSNs to revolutionize diverse sectors and improve quality of life remains vast and promising.

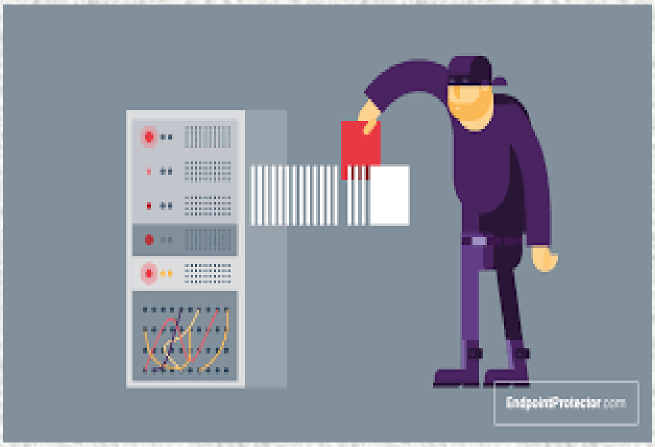
Chinmay Gawande(BE)

Threats to Information Security

In today's interconnected world, information security has become a paramount concern for individuals, businesses, and governments alike. The rapid advancement of technology has brought numerous benefits, but it has also created an environment where information is vulnerable to various threats. From malicious hackers to insider threats, the landscape of information security is complex and constantly evolving. In this article, we will explore some of the most significant threats to information security and discuss ways to mitigate them.

Cyberattacks, including hacking, are perhaps the most prevalent and immediate threats to information security. Hackers exploit vulnerabilities in computer systems, networks, and software to gain unauthorized access, steal sensitive data, disrupt operations, or infect systems with malware. Cyberattacks come in various forms, such as phishing, ransomware, and distributed denial of service (DDoS) attacks. Organizations must continuously update their cybersecurity measures to protect against these evolving threats.

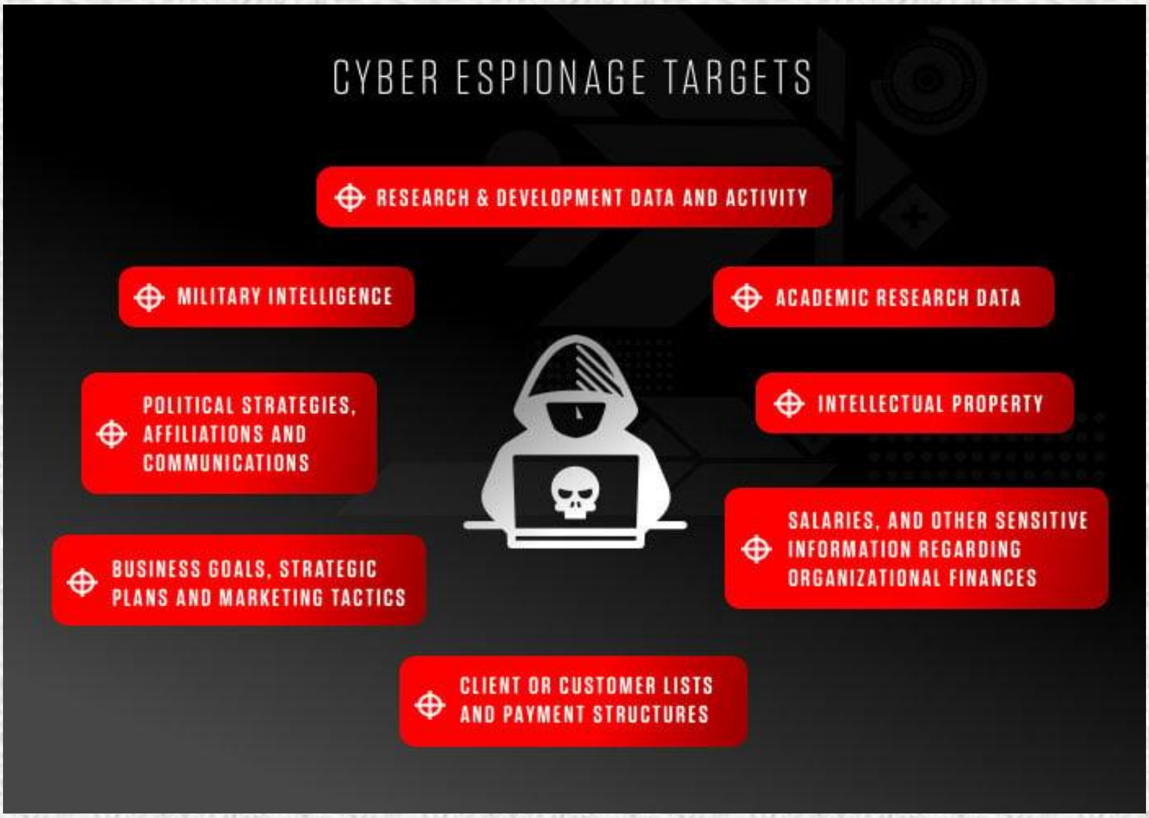
Malicious software, or malware, is a persistent menace. It includes viruses, Trojans, worms, and spyware. Ransomware, a specific type of malware, encrypts data and demands a ransom for its release. Malware can be introduced through infected emails, malicious downloads, or compromised websites. Regularly updating and patching software, educating users about safe online practices, and implementing robust antivirus solutions are essential steps to counter this threat.



While external threats are a significant concern, insiders with malicious intent can pose an equally grave risk to information security. Employees or trusted individuals can abuse their access to sensitive information for personal gain or to harm their organization. Mitigate this threat, organizations must implement strict access controls, monitor user activities, and foster a culture of security.

Social engineering involves manipulating individuals to reveal sensitive information or perform certain actions. Common tactics include pretexting (creating a fabricated scenario), baiting (enticing victims with something appealing), and phishing (using deceptive emails). Effective security awareness training and the use of multi-factor authentication can help protect against social engineering attacks. The Internet of Things (IoT) has brought a new dimension to information security concerns. As more devices become connected, they create additional entry points for cybercriminals. Unsecured IoT devices can be exploited to launch attacks or compromise data. Security measures, including device hardening, network segmentation, and firmware updates, are necessary to address this threat.

Data breaches, whether caused by cyberattacks or other factors, can have severe consequences. They lead to the exposure of sensitive information, such as personal and financial data, and can damage an organization's reputation. Encrypting data, regularly auditing systems, and promptly reporting breaches are key strategies for mitigating this threat.
APTs are prolonged and targeted cyberattacks typically carried out by well-funded and highly skilled adversaries. They aim to remain undetected for an extended period while continuously exfiltrating sensitive information. Combating APTs requires advanced threat detection capabilities, regular security assessments, and strong incident response plans.


CYBER ESPIONAGE TARGETS
RESEARCH & DEVELOPMENT DATA AND ACTIVITY
MILITARY INTELLIGENCE
ACADEMIC RESEARCH DATA
POLITICAL STRATEGIES, AFFILIATIONS AND COMMUNICATIONS
INTELLECTUAL PROPERTY
SALARIES, AND OTHER SENSITIVE INFORMATION REGARDING ORGANIZATIONAL FINANCES
BUSINESS GOALS, STRATEGIC PLANS AND MARKETING TACTICS
CLIENT OR CUSTOMER LISTS AND PAYMENT STRUCTURES

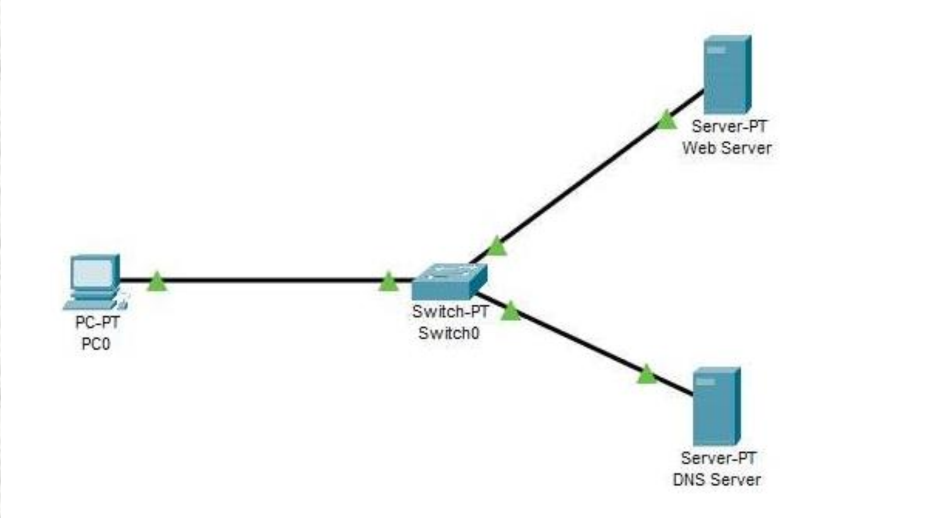
Supply chains are often overlooked but crucial components of an organization's information security. Third-party suppliers and vendors can inadvertently introduce vulnerabilities into an organization's systems. Regularly assessing and monitoring these relationships is essential to minimize this risk.

Information security is an ongoing battle, as new threats emerge and evolve. Understanding the diverse array of threats is the first step towards safeguarding valuable data and digital assets. It is crucial for organizations and individuals to remain vigilant, continually update security measures, and foster a culture of cybersecurity awareness to protect against the ever-present and ever-changing threats to information security in the digital age.

-Zhil Vora (BE EXTC)

HTTP / Web server - Configuration in Cisco Packet Tracer

DHCP is an Internet control protocol used to assign an IP address to any appliance, or node, on an internet network so they can transmit data using IP. DHCP automatically handles these configurations rather than requiring network administrators to manually set IP addresses to all network devices. DHCP can be executed on small local networks, as well as large company networks.



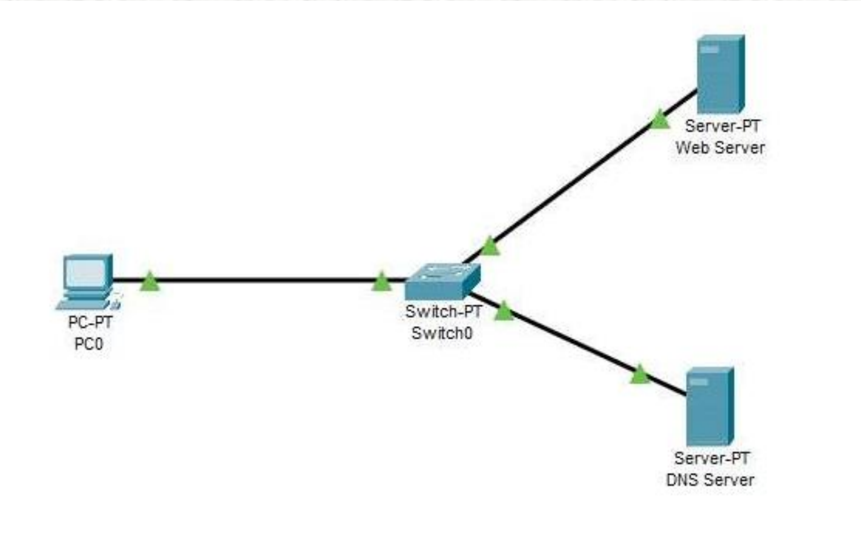
Steps:

Step 1: First, open the cisco packet tracer desktop and select the devices given below:

S.NO	Device	Model Name	Qty
1.	PC	PC	1
2.	switch	PT-switch	1
3.	server	Server-PT	2

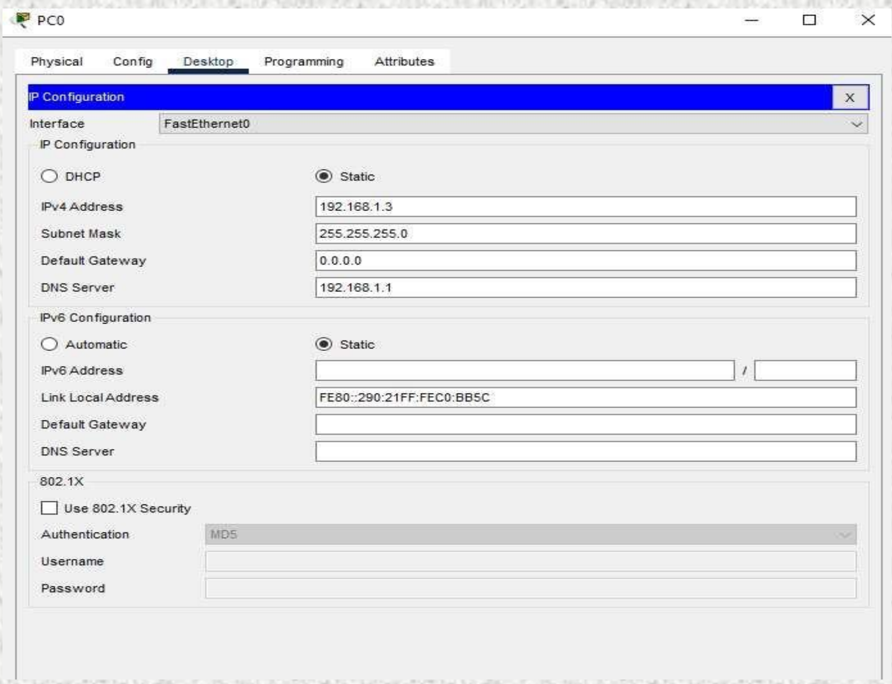
S.NO	Device	IPv4 Address	Subnet Mask	Default Gateway	DNS
1.	PC0	192.168.1.3	255.255.255.0	0.0.0.0	192.168.1.1
2.	Web Server	192.168.1.2	255.255.255.0	0.0.0.0	192.168.1.1
3.	DNS	192.168.1.1	255.255.255.0	0.0.0.0	192.168.1.1

- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.



Step 2: Configure the PCs (hosts) Web Server and DNS server with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address, click on the device.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Fill IPv4 address and subnet mask and other inputs.



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	192.168.1.1

IPv6 Configuration

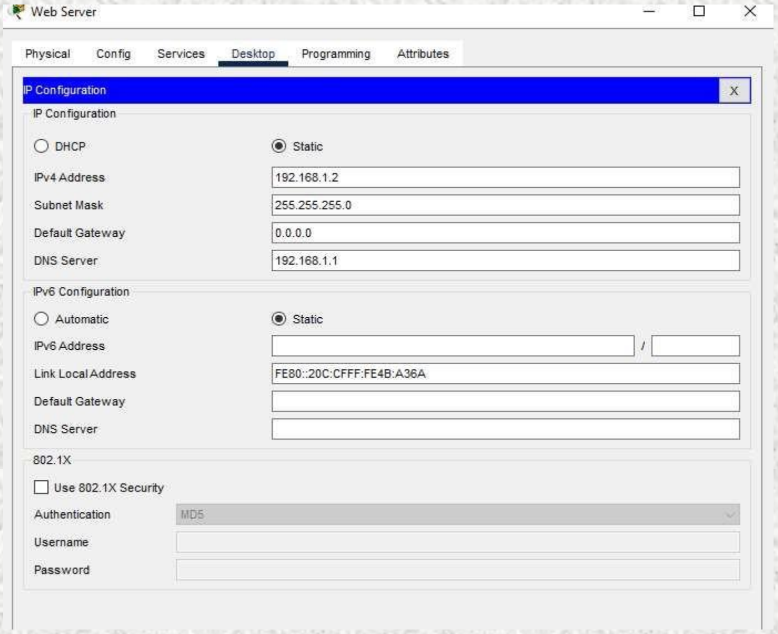
○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::290:21FF:FEC0:BB5C
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	



Web Server

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 192.168.1.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20C:CFFF:FE4B:A36A

Default Gateway:

DNS Server:

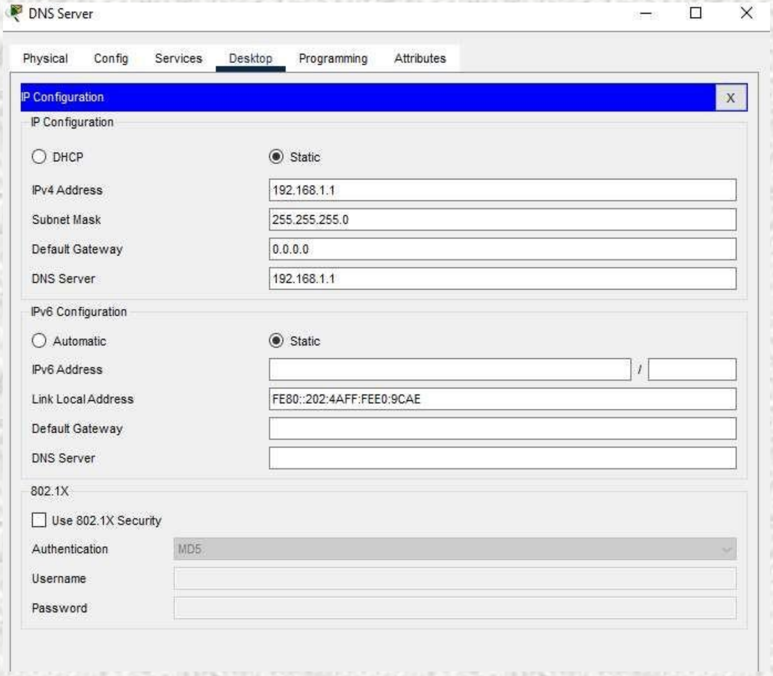
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:



DNS Server

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 192.168.1.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::202:4AFF:FEE0:9CAE

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

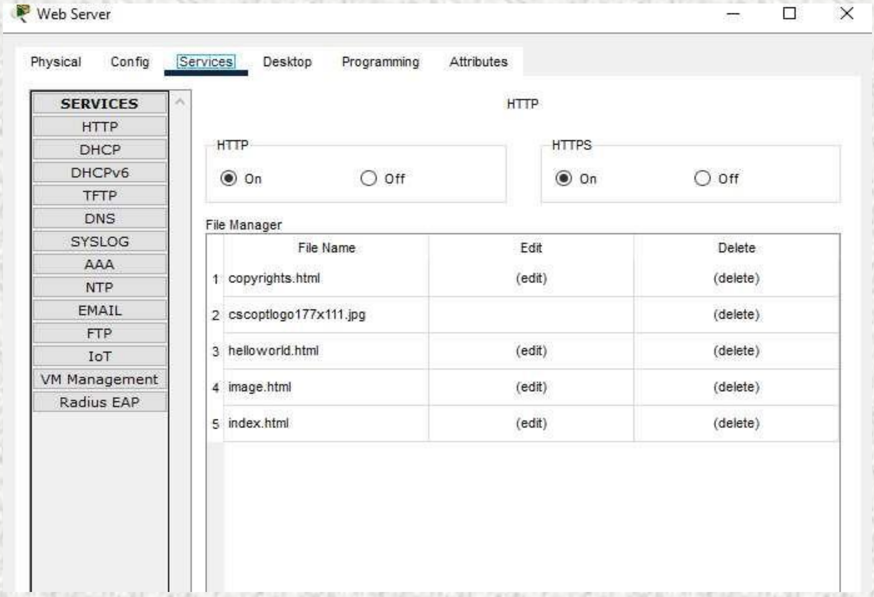
Authentication: MD5

Username:

Password:

Step 3: Configure the HTTP Web server

- To configure the HTTP server.
- Go to services then click on HTTP
- Then delete all of the files except the index. html and edit it.



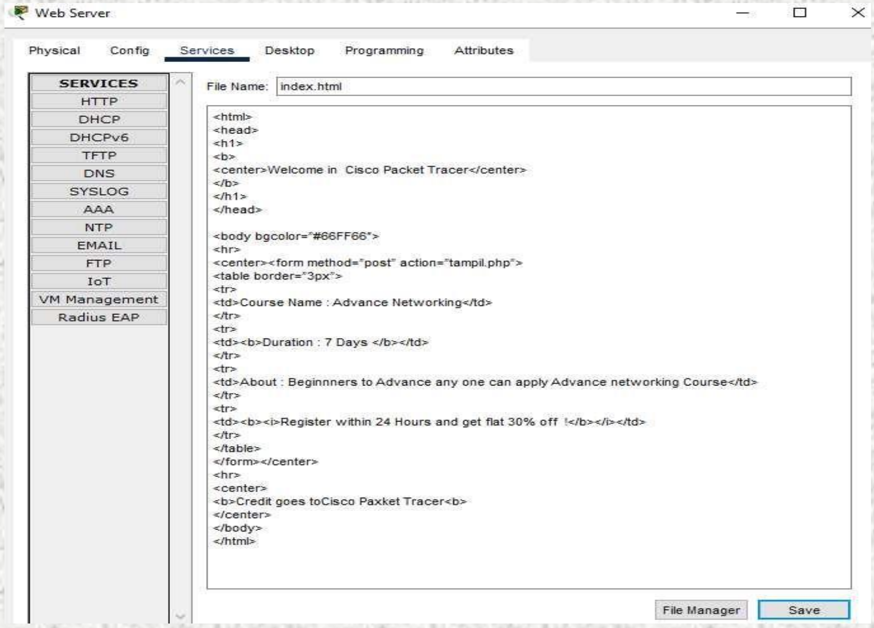
HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)



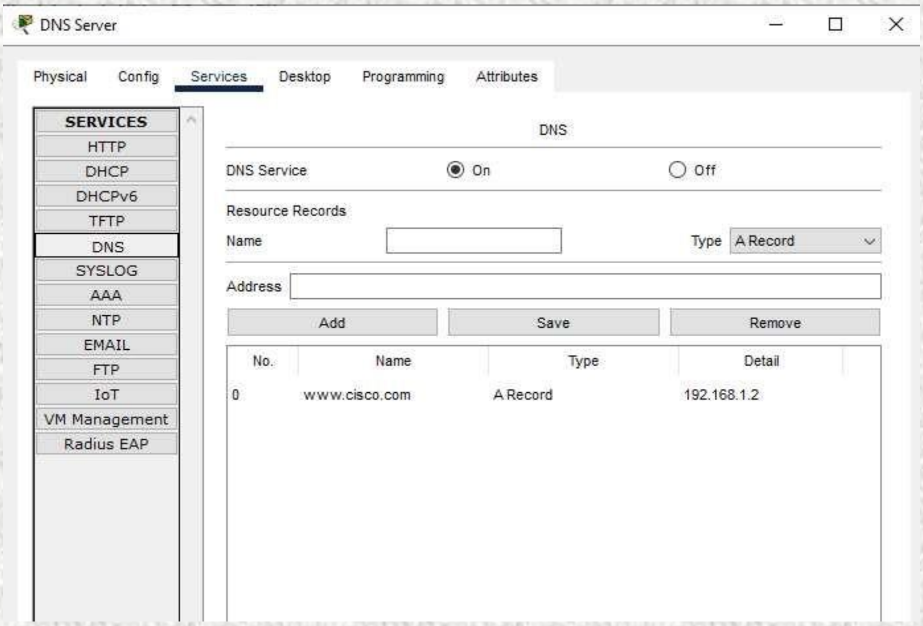
File Name: index.html

```
<html>
<head>
<h1>
<b>
<center>Welcome in  Cisco Packet Tracer</center>
</b>
</h1>
</head>

<body bgcolor="#66FF66">
<hr>
<center><form method="post" action="tampil.php">
<table border="3px">
<tr>
<td>Course Name : Advance Networking</td>
</tr>
<tr>
<td><b>Duration : 7 Days </b></td>
</tr>
<tr>
<td>About : Beginnners to Advance any one can apply Advance networking Course</td>
</tr>
<tr>
<td><b><i>Register within 24 Hours and get flat 30% off !</b></i></td>
</tr>
</table>
</form></center>
<hr>
<center>
<b>Credit goes toCisco Paxket Tracer<b>
</center>
</body>
</html>
```

Step 4: Configure the DNS server

- To configure the DNS server.
- Go to services then click on DNS.
- Then turn on the DNS services.
- Name the server cisco.com and type address 192.168.1.2 And add the record.



DNS

DNS Service ● On ○ Off

Resource Records

Name

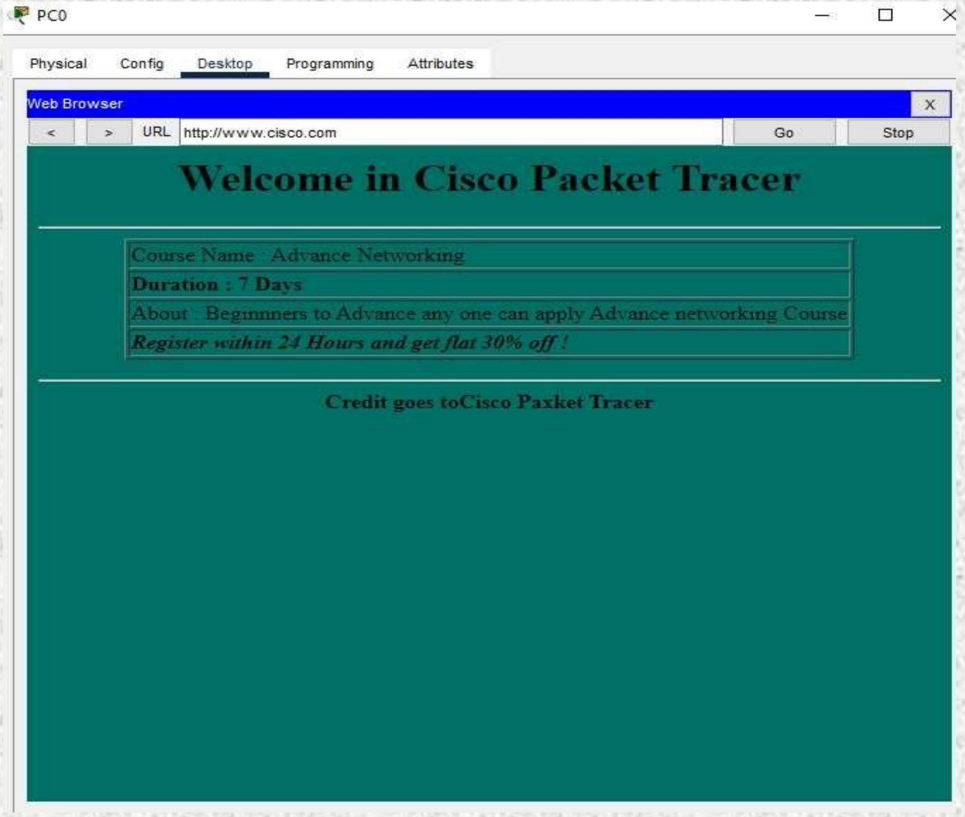
Type A Record

Address

No.	Name	Type	Detail
0	www.cisco.com	A Record	192.168.1.2

Step 5: Verify the server by using the web browser in the Host.

- Enter the IP address of Web server and click on GO.
- It will show the results.



URL http://www.cisco.com

Welcome in Cisco Packet Tracer

Course Name : Advance Networking
Duration : 7 Days
About : Beginnners to Advance any one can apply Advance networking Course
Register within 24 Hours and get flat 30% off !

Credit goes toCisco Paxket Tracer

Conclusion: Thus we have studied how to configure HTTP / Web Server.

Mihir Nawale(T.E)

Software Defined Networking (SDN)

Traditional Networks Vs. Software Defined Networking. Which is more beneficial and adaptable?

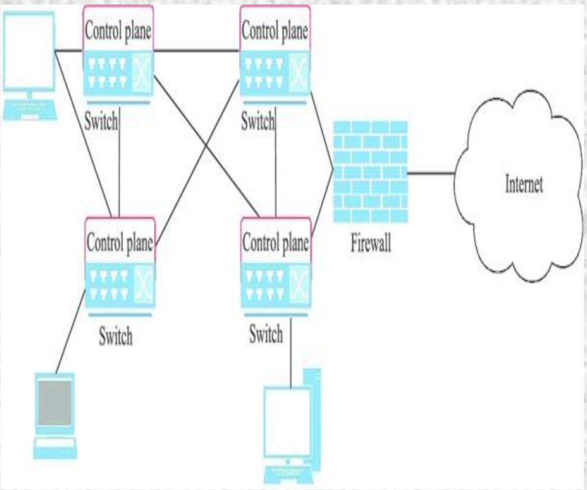


Fig. 1: Traditional Network Architecture

As technology is evolving daily, so our network's abilityis becoming more unreliable and difficult to maintain. Traditional networking in Internet communication systems refers to the use of physical cables and wires to transmit data between devices. This includes Ethernet cables, coaxial cables, and fiber optic cables. These networks are typically used in local area networks (LANs) and wide area networks (WANs) to connect devices such as computers, servers, and routers.

There are some limitations or drawbacks of traditional networks in Internet communication systems are:

a) Bandwidth limitations: Traditional networks have limited bandwidth, which can slow data transfer rates and degrade network performance.

b) Single Point of Failure: Traditional networks are often based on a centralized infrastructure, where failure of a single component or connection can affect the entire network.

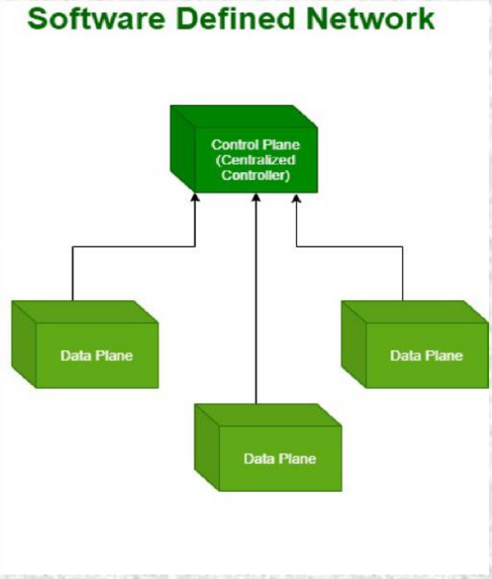
c) Scalability limitations: Traditional networks can face challenges in scaling to meet increasing network traffic and user demands.

d) Vulnerability: Traditional networks lack advanced security measures, which can make them vulnerable to security breaches and unauthorized access.

e) Lack of flexibility: Traditional networks have limited flexibility in adding or removing network components, making it difficult to adapt for changing needs.

f) Expensive Infrastructure: Traditional network infrastructure can be expensive to build and maintain, especially for large-scale deployments.

- **What is Software Defined Networking?**



Software-defined networking (SDN) is a networking approach that uses software-based controllers or application programming interfaces (APIs) to communicate with the underlying hardware infrastructure and route traffic on the network. This model differs from the traditional networking, which uses specialized hardware devices (such as routers and switches to control network traffic. SDN can create and control virtual networks through software or control traditional hardware. While network virtualization allows organizations to segment different virtual networks within a single physical network or connect devices on different physical networks to create a single virtual network, software find networks enabling new ways to control the routing of data packets through a central server.

Fig. 2: Software-Defined Networking

Why SDN is important?

SDN represents a substantial step forward from traditional networking, in which it enables:

✓ Increased control with greater speed and flexibility: In this, instead of manually programming multiple vendor-specific hardware devices, developers control the flow of traffic over a network by simply programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, it can choose a single protocol to communicate with any number of hardware device through a central controller.

✓ Customizable Network Infrastructure: With a software – defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. It allows network administrators to optimize the data flow through the network and prioritize applications which require more availability.

✓ Robust Security: A SDN network delivers visibility into entire network, providing a more holistic view of security threats. With proliferation of smart devices connecting with the internet, SDN has several advantages over traditional networks. Operators operate separate zones for devices which require different levels of security or needs to isolate compromised devices to prevent from infecting the rest networks.

The primary difference between SDN and traditional networks is the infrastructure of SDN. SDN is software-based, whereas the traditional networks are hardware-based. SDN is much more flexible as compared to traditional networks, as the control is software based. It also allows administrators to control the network, change configuration settings, provision resources, and increase the capacity all form a central user interface without requiring any additional hardware.

There are also some security differences SDN and traditional networks. Increased transparency and its ability to define secure paths helps SDN to provide better security in many ways. However, SDN uses a central controller, as it is important to maintain a secure network to secure the controller.

Architecture of SDN:

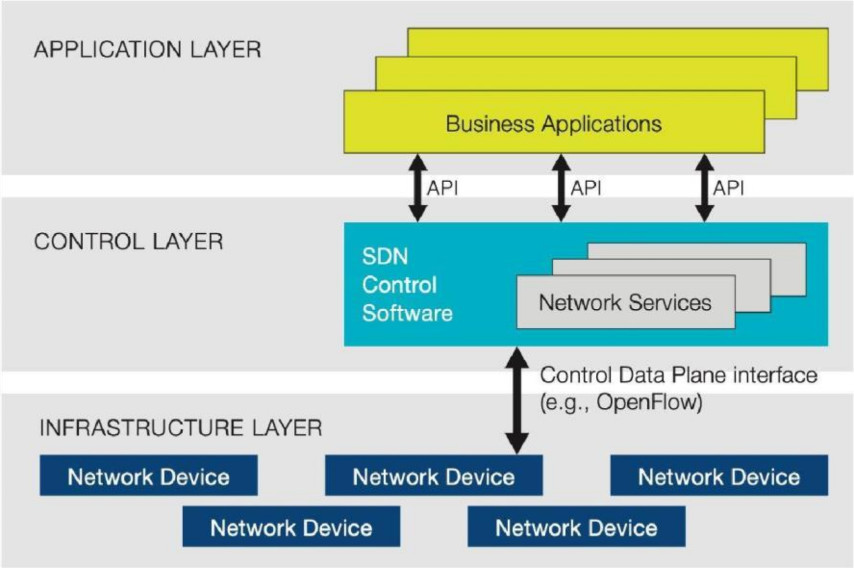


Fig. 3: Architecture of SDN

Software-Defined Networking (SDN) architecture consists of three main components:

A) Infrastructure Layer: It includes physical network devices such as switches, routers, and access points. It routes packets based on destination address.

B) Control Plane: The control plane is responsible for managing and controlling the operation of network devices. It consists of two main elements –

- Controller: It is the brain of the SDN architecture. It receives information about network topology, traffic, and policies from infrastructure devices. The instructions are also provided to the device for forwarding the packet.
- Southbound Interface: It connects the controller with the infrastructure devices. There are some protocols such as OpenFlow which is used to communicate and exchange information between controllers and devices.

C) Application Layer: This layer consists of various applications and services which uses the SDN architecture. These applications may be developed by the network administrators or any other developers to implement network management, security, traffic, engineering, and other functions.

Applications of SDN:

Some applications of SDN are

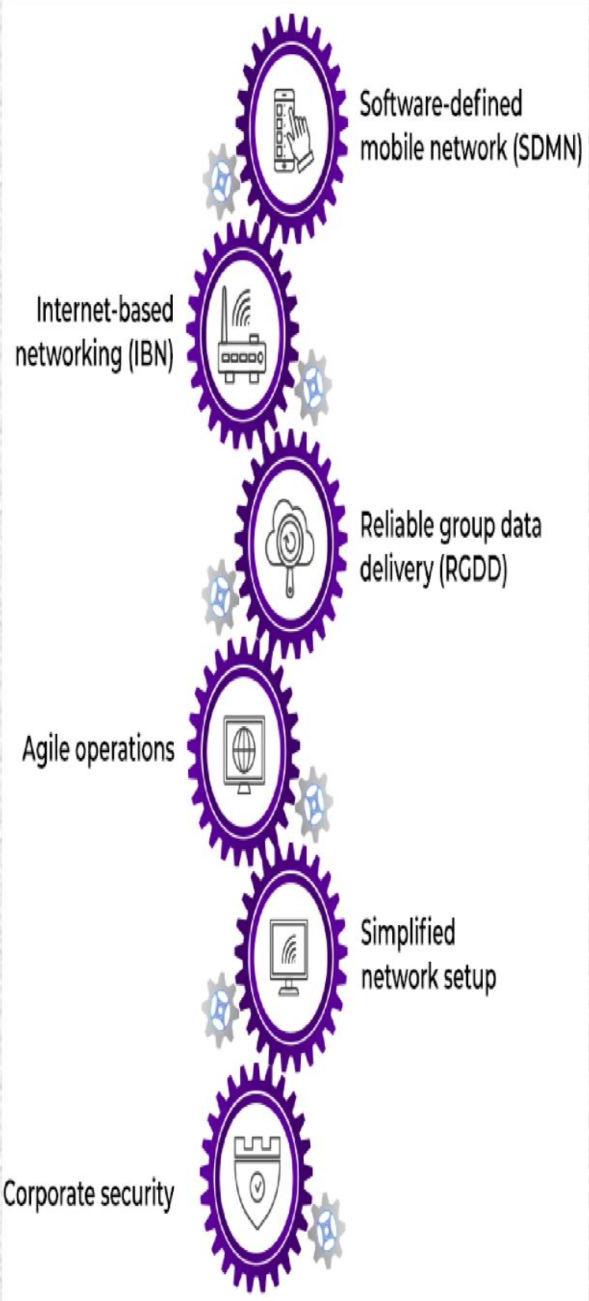

Software-defined mobile network (SDMN)
Internet-based networking (IBN)
Reliable group data delivery (RGDD)
Agile operations
Simplified network setup
Corporate security

Fig. 4: Applications of SDN

1) Network Virtualization: SDN enables the creation of virtual networks which can be dynamically deployed and managed. It enables efficient use of network resources and allows multiple virtual networks to be deployed on a single physical infrastructure.
2) Data Center Networking: SDN can simplify data center network management by providing a centralized control plane. It also enables dynamic allocation of network resources, increases network scalability, and facilitates automatic provisioning and orchestration of network services.
3) Wide Area Network (WAN): SDN can optimize WAN connectivity by dynamically routing traffic based on real-time network conditions. This enables efficient traffic engineering, bandwidth allocation, and quality of service (QoS) management in wide area networks.
4) Network Security: SDN can improve network security by enabling fine-grained control and monitoring of network traffic. It also allows you to implement security policies and access controls at a granular level, improving threat detection and responses.
5) Internet of Things (IoT): SDN provides scalable and flexible network management for IoT deployments. It enables efficient communication and coordination among IoT devices, facilitates device discovery and authentication, and allows for dynamic adaptation to changing IoT requirements.

Mihir Solanki(B.E.)

Free Space Optics and its Challenge

FSO is a communication system where free space acts as medium between transceivers and they should be in LOS for successful transmission of optical signal. Medium can be air, outer space, or vacuum. This system can be used for communication purpose in hours and in lesser economy. Although FSO systems can be a good solution for some broadband networking needs, there are limitations. Most significant is the fact that rain, dust, snow, fog, or smog can block the transmission path and shut down the network.

Introduction

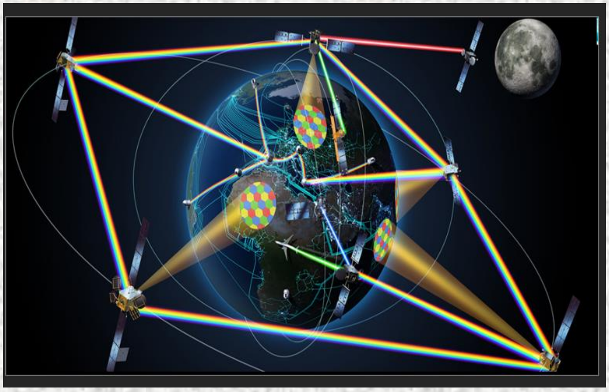
Free Space Optics Is Line Of Sight Technology Which Uses Laser And Photo Detector To Provide Optical Connection Between Two System Without Fiber. Fso Can Transmit Data, Audio And Video At The Speed Of 2.5ghz. Fso Uses Invisible Infrared Laser Light With Wavelength Of 750nm Or 1500nm. Fso Is Full Duplex. (It Can Transmits Data In Both Direction) FSO systems can function over distances of several kilometers. As long as there is a clear line of sight between the source and the destination, communication is theoretically possible. Even if there is no direct line of sight, strategically positioned mirrors can be used to reflect the energy. The beams can pass through glass windows with little or no attenuation

Why Free Space Optics

Free Space Optics Connectivity Doesn’t Require Expensive Fibre Optic Cable and Removes Need For Securing Spectrum Licenses For Radio Frequency Solutions.

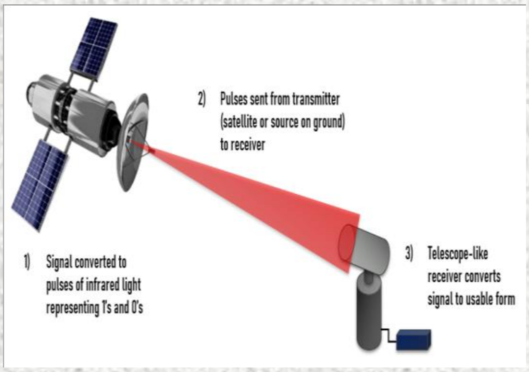
Backhaul: FSO can be used to carry cellular telephone traffic from antenna towers back to facilities wired into the public switched telephone network. Service acceleration: FSO can be also used to provide instant service to fiber-optic customers while their fiber infrastructure is being laid.

FSO Technology Requires Light. The Use Of Light Is A Simple Concept Similar To Optical Transmission Using Fiber Optics Cable.



How its work

FSO Technology Is Based On Connectivity Between Fso Based Optical Wireless Units Each Consisting Of An Optical Tranceiver with A Transmitter And A Receiver To Provide Full-duplex (BI- DIRECTIONAL) Capability. Each Optical Wireless Unit Uses an Optical Source, Plus A Lens Or Telescope That Transmitts Light Through The Atmosphere To Another Lens Receiving The Information, At This Point The Receiving Lens Or Telescope Connects To A High-sensitivity Receiver Via Optical Fiber.


2) Pulses sent from transmitter (satellite or source on ground) to receiver
1) Signal converted to pulses of infrared light representing 1's and 0's
3) Telescope-like receiver converts signal to usable form

Challenges

- Weather Severity At Which FSO Signal Attenuation Can Be Impacted:- Rain At 6 Inches Per Hour, Wet Snow Rate Of 4 Inches Per Hour. Dry Snow Rate of 2 Inches Per Hour. Fog with Visibility of < 6% Of The Transmission Distance.
- Physical Obstructions: - Birds Can Temporarily Block the Beam, But This Tends to Cause Only Short Interruptions and Transmissions Are Easily Resumed.
- Building sway/seismic activity: - The movement of buildings can upset receiver and transmitter alignment. Light Pointe's FSO-based optical wireless offerings use a divergent beam to maintain connectivity. When combined with tracking, multiple beam FSO-based systems provide even greater performance and enhanced installation simplicity.
- Safety: - Safety of The Lasers Does Not Depend On Its Frequency, But Rather On The Classification Of The Laser. There Are Two Primary Classification Bodies, The CDRH and The IEC. Commercial Systems On the Market Today Are Compliant with Both Standards.

Conclusion

FSO offers many advantages over existing techniques which can be either optical or radio or microwave. Less cost and time to setup are the main attraction of FSO system. Optical equipment can be used in FSO system with some modification. Merits of FSO communication system and its application are a make it a hot technology but there are some problems arising due to the attenuation caused by medium.

Sunny Pawar(B.E.)