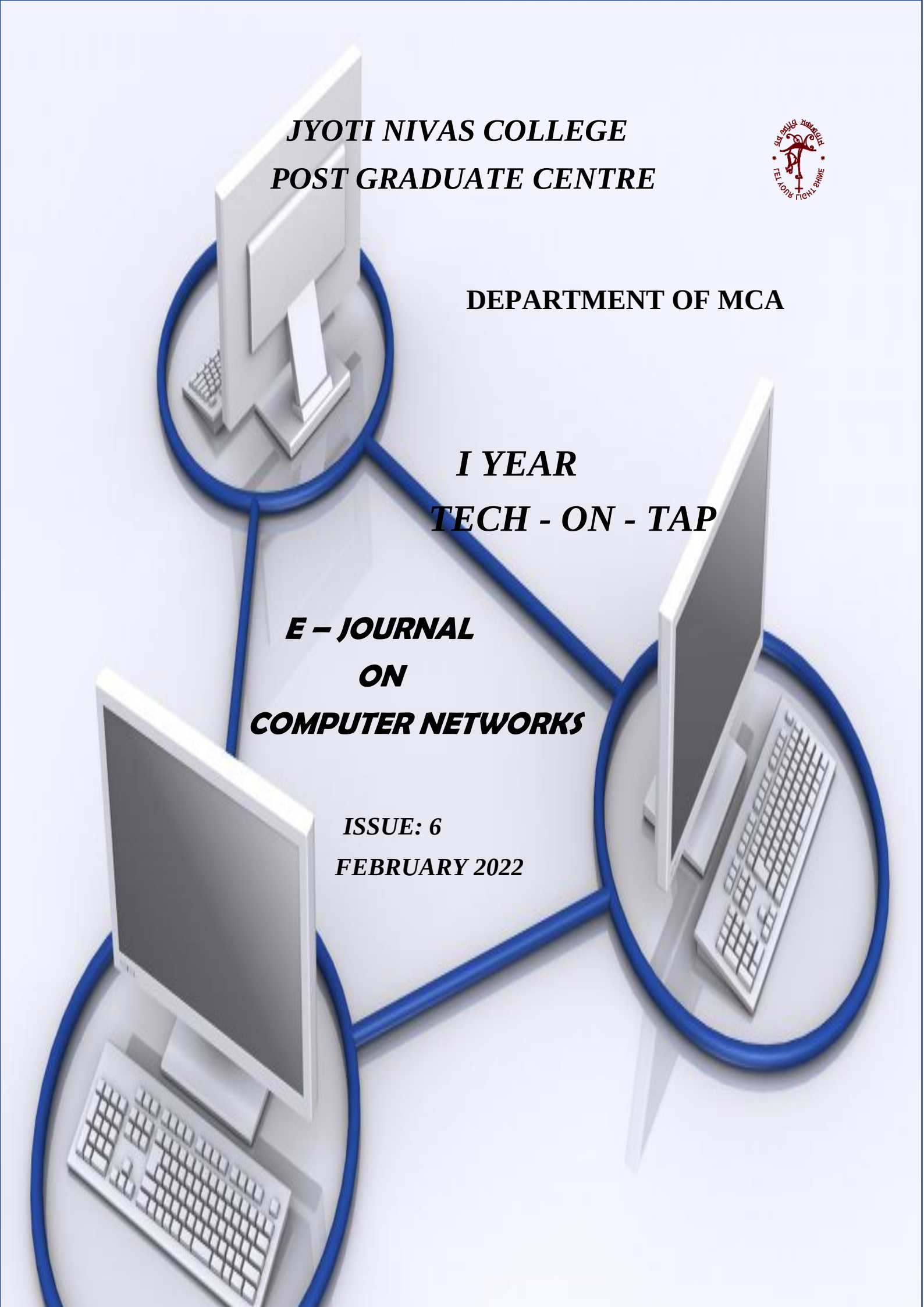


JYOTI NIVAS COLLEGE

POST GRADUATE CENTRE

DEPARTMENT OF MCA

I YEAR

TECH - ON - TAP

E – JOURNAL

ON

COMPUTER NETWORKS

ISSUE: 6

FEBRUARY 2022

STEGANOGRAPHY

CHITHRA A(21MCA12)

VANDANA R(21MCA44)

Steganography is the technique to encryption and decryption. It contains message within another message r a physical object. In computing or electronic contexts, a computer file, message, image, video is concealed within another file. Message, image, or video.

ADVANTAGES OF THIS TECHNOLOGY

The main advantages of steganography over cryptography alone is that the intended secret message doesn't attract attention to itself as an object of scrutiny. Plainly visible encrypted message, no matter how unbridle they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

Whereas includes the concealment of information within within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

HOW IT WORKS?

1.Hiding a message in the title and context of a shared video or image.

2.Misspelling names or words that is popular in the media in a given week, to suggest an alternate meaning.

3.Hiding a picture that can be traced by using Paint or any other drawing tool

Reference: **https://www.merriam-webster.com/dictionary/steganography**

https://en.wikipedia.org/wiki/Steganography#:~:text=Steganography%20can%20be%20used%20for,as%20in%20the%20EURion%20constellation).

MEDIA GATEWAY CONTROL PROTOCOL

MEGHANA N (15MCA24)

PRERANA D SALIGRAM (21MCA29)

The **Media Gateway Control Protocol** (**MGCP**) is a signaling and call control communications protocol used in voice over IP (VoIP) telecommunication systems. It implements the media gateway control protocol architecture for controlling media gateways connected to the public switched telephone network (PSTN). The media gateways provide conversion of traditional electronic media to the Internet Protocol (IP) network. The protocol is a successor to the Simple Gateway Control Protocol (SGCP), which was developed by Bellcore and Cisco, and the Internet Protocol Device Control (IPDC).

The methodology of MGCP reflects the structure of the PSTN with the power of the network residing in a call control center softswitch which is analogous to the central office in the telephone network. The endpoints are low-intelligence devices, mostly executing control commands from a call agent or media gateway controller in the SoftSwitch and providing result indications in response. The protocol represents a decomposition of other VoIP models, such as H.323 and the Session Initiation Protocol (SIP), in which the endpoint devices of a call have higher levels of signaling intelligence.

MGCP is a text-based protocol consisting of commands and responses. It uses the Session Description Protocol (SDP) for specifying and negotiating the media streams to be transmitted in a call session and the Real-time Transport Protocol (RTP) for framing the media streams.

References: Wikipedia

Ribboncommunications

CLOUD ROBOTICS

BUDDI.NAGA SAI LOHITHA (21MCA09)

HARSHITHA PATIL (21MCA19)

HISTORY

The term "Cloud Robotics" first appeared in the public lexicon as part of a talk given by James Kuffner in 2010 at the IEEE/RAS International Conference on Humanoid Robotics entitled "Cloud-enabled Robots". Since then, "Cloud Robotics" has become a general term encompassing the concepts of information sharing, distributed intelligence, and fleet learning that is possible via networked robots and modern cloud computing.

The term "cloud computing" was popularized with the launch of Amazon EC2 in 2006. It marked the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization and service-oriented architecture.

INTRODUCTION

Cloud robotics is an intersection between robotics, cloud computing, deep learning, big data, and internet of things, and other emerging technologies. It is a field of robotics where robots rely on the internet network to implement their functions. More like, a robot whose sensing and computation are not integrated into a single system, thus robot having “an extended or a shared brain”. As a result, robots are getting not only smarter by connecting to the cloud, but also cheaper and smaller!

COMPONENTS

- Offering a global library of images, maps, and object data, often with geometry and mechanical properties, expert system, knowledge base (i.e. semantic web, data centres) ;
- Massively-parallel computation on demand for sample-based statistical modelling and motion planning, task planning, multi-robot collaboration, scheduling and coordination of system
- Robot sharing of outcomes, trajectories, and dynamic control policies and robot learning support
- Human sharing of "open-source" code, data, and designs for programming, experimentation, and hardware construction
- On-demand human guidance and assistance for evaluation, learning, and error recovery
- Augmented human–robot interaction through various way (Semantics knowledge base, Apple SIRI like service etc.).

APPLICATIONS

1. Autonomous mobile robots
2. Cloud medical robots
3. Assistive robots
4. Industrial robots

LIMITATIONS

- Controlling a robot's motion which relies heavily on (real-time) sensors and feedback of controller may not benefit much from the cloud.
- Tasks that involve real-time execution require on-board processing.
- Cloud-based applications can get slow or unavailable due to high-latency responses or network hitch. If a robot relies too much on the cloud, a fault in the network could leave it "brainless."

RISKS

- Environmental security
- Data privacy and security
- Ethical problems

REFERENCES

- "Cloud Robotics and Automation A special issue of the IEEE Transactions on Automation Science and Engineering". IEEE. Archived from the original on 14 September 2017. Retrieved 7 December 2014.
- "RoboEarth". Archived from the original on 2014-12-01. Retrieved 2014-12-07.
- Goldberg, Ken. "Cloud Robotics and Automation"

VOICE OVER INTERNET PROTOCOL- VoIP

ARUNODYA P (21MCA06)

RENUKA M (21MCA35)

VoIP is an acronym for Voice over Internet Protocol that describes the method to place and receive phone calls over the internet. Most people consider VoIP the alternative to the local telephone company.

IP address is Internet Protocol address. An IP address is how computers and devices communicate with each other on the internet.

VoIP service providers do more than establishing calls. They perform routing of outgoing and incoming calls through existing telephone networks. Landlines and cell phones depend on the Public Switched Telephone Network (PSTN).

A VoIP phone system facilitates calls between other phones or over to another telephone company. It also provides other useful functions like voicemail, call forwarding, call recording, and more.

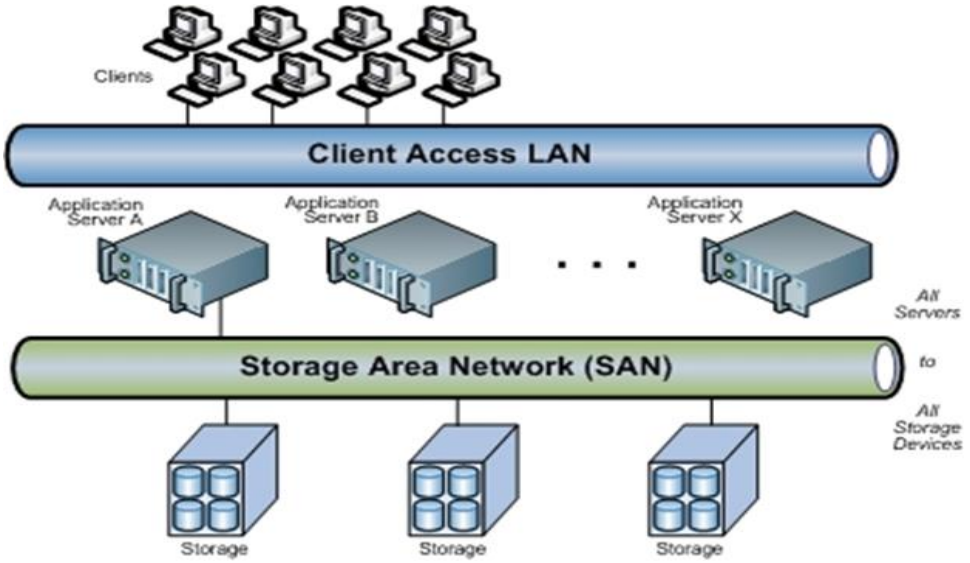
SAN (STORAGE AREA NETWORK)

HEMA N(21MCA20)

PRIYANKA N(21MCA32)

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs may also span multiple sites.

A SAN presents storage devices to a host such that the storage appears to be locally attached. This simplified presentation of storage to a host is accomplished through the use of different types of virtualization.



SANs are often used to:

- Improve application availability (e.g., multiple data paths)
- Enhance application performance (e.g., off-load storage functions, segregate networks, etc.)
- Increase storage utilization and effectiveness (e.g., consolidate storage resources, provide tiered storage, etc.), and improve data protection and security.
- SANs also typically play an important role in an organization's Business Continuity Management (BCM) activities.

SANs are commonly based on Fibre Channel (FC) technology that utilizes the Fibre Channel Protocol (FCP) for open systems and proprietary variants for mainframes. In addition, the use of Fibre Channel over Ethernet (FCoE) makes it possible to move FC traffic across existing high speed Ethernet infrastructures and converge storage and IP protocols onto a single cable. Other technologies like Internet Small Computing System Interface (iSCSI), commonly used in small and medium sized organizations as a less expensive alternative to FC, and InfiniBand, commonly used in high performance computing environments, can also be used. In addition, it is possible to use gateways to move data between different SAN technologies.

LIFI TECHNOLOGY

AMRITHA BALAKRISHNAN (21MCA02)

FEBA BIJU (21MCA1)

Transmission of data is one of the most important days to day activities in the fast-growing world. The current wireless networks that connect us to the Internet are very slow when multiple devices are connected. Also, with the increase in the number of devices which access the Internet, the availability of fixed bandwidth makes it much more difficult to enjoy high data transfer rates and to connect a secure network. Li-Fi stands for Light Fidelity. The technology was proposed by the German physicist Harald Haas in 2011 TED (Technology, Entertainment, Design) Global Talk on Visible Light Communication (VLC). Li-Fi is a wireless optical networking technology that uses light emitting diodes (LEDs) for transmission of data.

ADVANTAGES OF Li-Fi:

Li-Fi, which uses visible light to transmit signals wirelessly, is an emerging technology poised to compete with Wi-Fi. Also, Li-Fi removes the limitations that have been put on the user by the Radio wave transmission such as Wi-Fi. Advantages of Li-Fi technology include:

a) Efficiency: Energy consumption can be minimised with the use of LED illumination which are already available in the home, offices and Mall etc

b) High speed: Combination of low interference, high bandwidths and high-intensity output, help Li-Fi provide high data rates i.e. 1 Gbps or even beyond.

c) Availability: Availability is not an issue as light sources are present everywhere. Wherever there is a light source, there can be Internet. Light bulbs are present everywhere – in homes, offices, shops, malls and even planes, which can be used as a medium for the data transmission.

d) Cheaper: Li-Fi not only requires fewer components for its working, but also uses only a negligible additional power for the data transmission.

e) Security: One main advantage of Li-Fi is security. Since light cannot pass through opaque structures, Li-Fi internet is available only to the users within a confined area and cannot be intercepted and misused, outside the area under operation.

f) Li-Fi technology has a great scope in future.

LIMITATION OF Li-Fi:

Some of the major limitations of Li-Fi are:

- Internet cannot be accessed without a light source. This could limit the locations and situations in which Li-Fi could be used.
- It requires a near or perfect line-of-sight to transmit data
- Opaque obstacles on pathways can affect data transmission
- Natural light, sunlight, and normal electric light can affect the data transmission speed
- Light waves don't penetrate through walls and so Li-Fi has a much shorter range than Wi-Fi
- High initial installation cost, if used to set up a full-fledged data network.
- Yet to be developed for mass scale adoption.

FUTURE SCOPE:

The concept of Li-Fi is deriving many people as it is free (require no license) and faster means of data transfer. If it evolves faster, people will use this technology more and more.

REFRENCES:

Microsoft Word - lifi study paper - approved.docx (tec.gov.in)

http://www.warse.org/pdfs/2014/icetetssp25.pdf

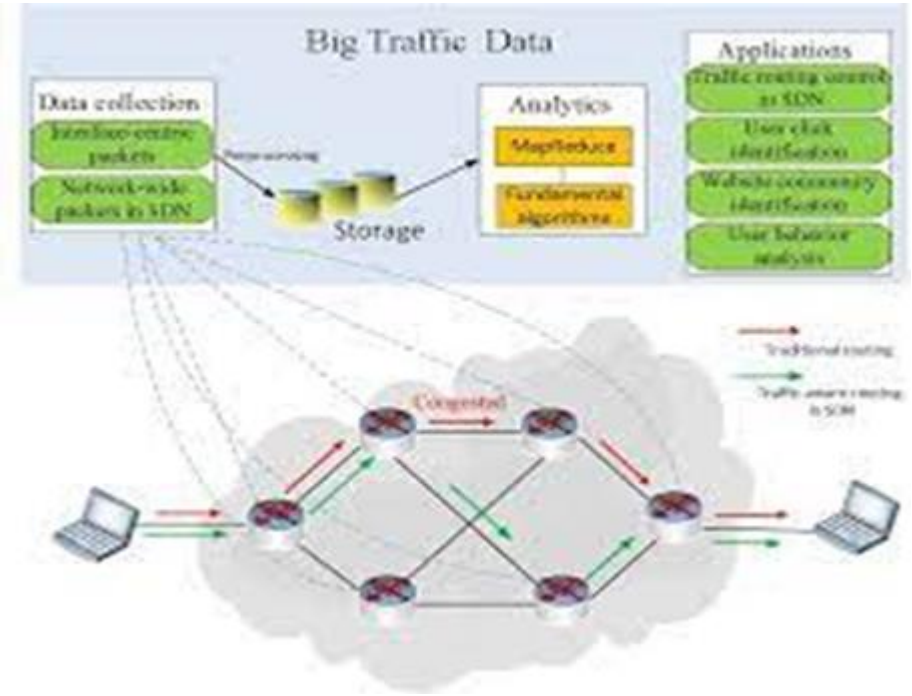
BIG DATA ANALYTICS IN MOBILE CELLULAR NETWORKS

VAISHNAVI P(21MCA43)

RAKSHITHA J (21MCA34)

Mobile cellular networks have become both the generators and carriers of massive data. Big data analytics can improve the performance of mobile cellular networks and maximize the revenue of operators. Recent years have witnessed tremendous advances in wireless cellular networks. With recent advances of wireless technologies and ever-increasing mobile applications, mobile cellular networks have become both generators and carriers of massive data. When Geo-locating mobile devices, recording phone calls, and capturing mobile applications' activities, an enormous amount of data is generated and carried in mobile cellular networks.

Historically, the massive data in mobile cellular networks hasn't been paid much attentions. With data constantly accumulated in the database and the technologies of big data analytics rapidly developed, the great value hided behind data has gradually been revealed. It is desirable to make good use of this precious resource, big data, to improve the performance of mobile cellular networks and maximize the revenue of operators. Traditional data analytics shows its in-adequateness when encountered with the big cellular data. First, traditional data analytics deals with structured data. The large amount of App-based data is, however, generally unstructured. Second, the implementation of data analysis is traditionally confined within a department, or a business unit. The final analytical conclusions come from very limited, local angles, rather than global perspectives. Third, the analytics mainly aims at transaction data, and pays less attention to the operational data, due to its incapability to make real-time decisions.



Big data analytics can extract much more insightful information than traditional data analytics, and can help improve the performance mobile cellular networks and maximize the revenue of

operators [5]. For example, the complete data related to a subscriber is usually fragmented in different business departments. Big data analytics is capable of collecting the scattered data to understand the user behavior and preferences from multiple perspectives to portray an integrated picture. Moreover, subscribers' living habits and the timetable can be generally inferred from the usage of traffic over different time periods of a day; their surfing habits and interests can be roughly obtained from the logs; their frequently visited places or the range of activities can be approximately derived from home location register (HLR) databases. Another significant feature of big data analytics is real-time processing. With big data analytics, operators can monitor their infrastructure in real-time, and make autonomous and dynamic decisions.

Despite the potential vision of big data analytics in mobile cellular networks, many significant research challenges remain to be addressed before the widespread deployment of big data analytics in mobile cellular networks. In particular, there is data confidentiality issue for the purpose of subscribers' privacy-preserving and security-protection. Mobile cellular networks have large amount of sensitive personal information, such as subscriber's names, ID numbers, physical locations, images files, top contacts, passwords, etc. If operators fail to leverage big data in a proper way, big data analytics will bring privacy/security issues to mobile cellular networks. In addition, as mobile cellular networks have scarce bandwidth, how to filter out un-useful data and compress/transmit useful data presents significant challenges to the design of mobile cellular networks.

Five Key Types of Big Data Analytics:

i. Prescriptive Analytics
ii. Diagnostic Analytics
iii. Descriptive Analytics
iv. Predictive Analytics
v. Cyber Analytics

Big data analytics will be an indispensable part of the mobile cellular operators' consideration of network operation, business deployment, and even the design of the next-generation mobile cellular network architectures.

References:

https://ieeexplore.ieee.org/document/7429688

NETWORK SIMULATOR

PRITY KUMARI (21MCA30)

RUPA KUMARI (21MCA36)

Network Simulator is a tool used for simulating the real-world network on one computer by writing scripts in C++ or Python. Normally if we want to perform experiments, to see how our network works using various parameters. We don't have number of computers and routers for making different topologies.

So, to overcome these drawbacks we use NS3, which is a discrete event network simulator for Internet. NS3 helps to create various virtual nodes (i.e., computers in real life) and with the help of various Helper classes it allows us to install devices, internet stacks, application, etc. to our nodes.

Using NS3 we can create Point-To-Point, Wireless, CSMA (Carrier Sense Multiple Access), etc. connections between nodes. Point-To-Point connection is same as a LAN connected between two computers. Wireless connection is same as Wi-Fi connection between various computers and routers. CSMA connection is same as bus topology between computers. After building connections we try to install NIC (Network Interface Card) to every node to enable network connectivity.

Most of the commercial Simulators are GUI driven, while some network simulators are Command Line Argument (CLI) driven. The network configuration describes the network (nodes, routers, switches, links) and the events (data transmissions, packet error, etc.). Output results would include network-level metrics, link metrics, device metrics etc. Further, drill down in terms of simulations trace files would also be available. Trace files log every packet, every event that occurred in the simulation and is used for analysis.

Simulators come with support for the most popular technologies and networks in use today such as 5G, Internet of Things (IoT), Wireless LANs, Mobile ad hoc network, Wireless Sensor Network, Vehicular ad hoc networks, Cognitive radio networks, LTE etc.

References :- https://en.wikipedia.org , https://www.geeksforgeeks.org

WIRELESS SENSOR NETWORKS

G. SATWIKA (21MCA17)

ASHIYA MEHAK (21MCA01)

ABSTRACT

The paper presents introduction, advantages and disadvantages, possible applications and research challenges of Wireless Sensor Networks (WSN).

Introduction to Wireless Networks

A Wireless network is any sort of computer network that uses wireless data connection to plug network nodes. Wireless networks are computer networks who are not connected by cables regardless of the sort. The use of a wireless networks enables enterprises to prevent the costly means of introducing cables into buildings or as a connection between different equipment locations. The cornerstone of wireless systems is radio waves, an implementation that occurs at the physical higher level of network structure.

CONCLUSION

WSN follows different topologies such as star, tree, mesh, hybrid etc. Hence one can understand pros and cons of these topologies to derive advantages of WSN and disadvantages of WSN.

Reference

https://www.researchgate.net/figure/The-structure-of-Wireless-sensor-Network_fig1_287935513

WIRELESS TECHNOLOGY ZIGBEE

UMA BHUVANESHWARI K V (21MCA42)

MYTHREYI S N (21MCA25)

CONTENT:

- INTRODUCTION
- ARCHITECTURE
- ADVANTAGES
- DISADVANTAGES
- FUTURE SCOPE
- CONCLUSION

INTRODUCTION:

ZigBee is a new wireless technology

Technological Standard Created for Control and Sensor Networks

Based on the IEEE 802.15.4 Standard

Created by the ZigBee Alliance

Philips, Motorola, Intel, HP are all members of the Alliance.

ARCHITECTURE:

Layered architecture

These layers facilitate the features that make ZigBee very attractive:

1. low cost
2. easy implementation
3. reliable data transfer
4. short-range operations
5. very low power consumptions
6. adequate security features

ZIGBEE ADVANTAGES:

The zig-bee has flexible network structure

- has a very long battery life.
- It is low power consumption.
- It is easy to install.
- It can be easily implemented.
- It supports large number of nodes i.e., 6500 nodes approximately

Disadvantages of ZIGBEE:

- It is so highly risky to be used for official private information.
- The Zig-bee has low transmission rate.

- Replacement with Zig-bee compliant appliances can be costly.
- It does not have many end devices available yet.

FUTURE SCOPE:

- Zigbee has very promising future in front of it.
- It leads to cheap wireless technology, so that it can be widely used for low-rate data transfer.
- Zigbee aims to achieve greater efficiency

CONCLUSION:

Zigbee has been developed to meet the growing demand for capable wireless networking between numerous low-power devices.

These networks are easy to deploy which is cheaper as compared to other technologies

Used for campus-wide electrical and security systems from a single computer

Zig-bee networks can be configured and operate in many different and often substle ways.

REFRENCE:

1. **https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/**
- Internet

D2D COMMUNICATION IN 5G NETWOKS

DEVIKA K (21MCA13)

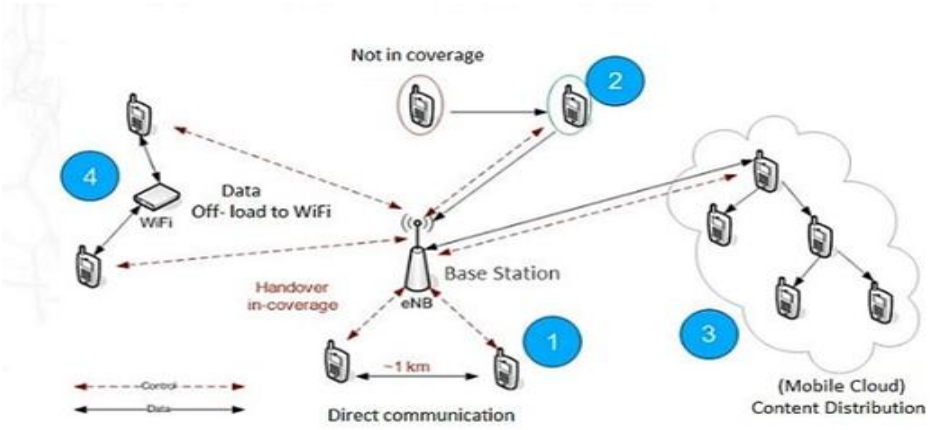
JHANCY S (21MCA22)

INTRODUCTION

Direct Device-to-Device (D2D) communication, which refers to direct communication between devices (i.e. users) without data traffic going through any infrastructure node, has been widely foreseen to be an important cornerstone to improve system performance and support new services beyond 2020 in the future fifth generation (5G) system.

WORKING

Device to device communication can be achieved in multiple modes of operation depends on the scenarios. According to the situation, most suitable operation mode will be chosen to establish efficient transmission.



Scenario 1: If two devices are in proximity they can start communication like sharing data. This helps to improve data rate, reduce power consumption of devices and total load reduction of base stations. The control will be handled by base station.

Scenario 2: During the absence of an active mobile network connection or insufficient signal reception, D2D enabled devices can establish an alternative communication interface

D2D enabled devices can establish an alternative communication interface with its surrounding devices which are connected mobile base stations. It will help the node with no coverage to maintain a connection to the mobile network.

Scenario 3: Multiple devices can connect to a device which has an active connection to base station and further extend this network with adding connection to more devices. All devices in this small mobile cloud will receive same data in the form of advertising or messages from the source.

Scenario 4: In this case, multiple devices are offloaded to Wi-Fi data connection for communication. Control signals to devices (UE) will be handled by the base station. Wi-Fi offloading offers much higher data rate, less power consumption and avoid traffic overload of base stations.

SIGNIFICANCE IN FUTURE APPLICATIONS

5G technology will make use of D2D communication for wide range of applications. Internet of Things will connect billions smart things (devices and sensors) to internet. D2D communication can be implemented in IoT applications for low power mesh networking and smart sensor clouds

LIMITATIONS

Complex algorithms required to efficiently handle devices without interference. Signal transmission power to a particular device need to be increased from base station to overcome surrounding interference.D2D communication is a proximity based protocol, thus distance between devices are limited due to power requirement.

REFERENCES

https://www.rfpage.com

https://www.cambridge.org

GREEN NETWORKING

AVULA LAKSHMI (21MCA08)

JAISRI D(21MCA21)

WHAT IS GREEN NETWORKING?

Green Networking is a broad term used to cover a number of different techniques for reducing power consumption in networking hardware and appliances.

HOW CAN IT BE IMPLEMENTED?

Once a decision has been made to “go green”, there are three Major ways that a company can implement green technologies and begin harvesting benefits.

DEVICE EFFICIENCY

The strategy to behind efficiency is simple. It involves replacing aging hardware with newer models designed consume less power. Again, network equipment, such as bridges and routers, can suck up a significant amount of power.

VIRTUAL COMPUTING

With virtual networking, one server can take the place of multiple test servers, cutting down on earth consumption.

CLOUD SERVICES

As with green networking,” cloud” is another buzzword making the rounds these days. It seems like everyone wants to move to the cloud, and for a green reason.

GOALS OF GREEN NETWORKING

i)Reduction of energy consumption.

ii)Improvement of energy efficiency

REFERENCES:

1.Scott Calonico.”Green Networking”.

2.Gartner,” Green IT: the new industry shock wave” November 2007. [5] “SMART” 2020: enabling the love carbon economy

CONTENT DELIVERY NETWORK

C SHALINI REDDY (21MCA11)

SHILPA V (21MCA39)

A content delivery network (CDN) is a group of geographically distributed servers that speed up the delivery of web content by bringing it closer to where users are. Data centers across the globe use caching, a process that temporarily stores copies of files, so that you can access internet content from a web-enabled device or browser more quickly through a server near you. CDNs cache content like web pages, images, and video in proxy servers near to our physical

location. This allows us to do things like watch a movie, download software, check your bank balance, post on social media, or make purchases, without having to wait for content to load.

The mission of a CDN is to reduce latency. Latency is that annoying delay we experience when trying to access a web page or video stream before it fully loads on our device. Although measured in milliseconds, it can feel like forever, and may even result in a load error or time-out. Some content delivery networks alleviate latency by reducing the physical distance that the content needs to travel to reach you. Therefore, larger, more widely distributed CDNs are able to deliver web content more quickly and reliably by putting the content as close to the end user as possible.

CDN provides house cached content in either their own network points of presence (POPs) or in third-party data centers. When a user requests content from a website, if the content is cached on a CDN, it redirects the request to the server nearest to the user and delivers the cached content from its location at the network edge. This process is invisible to the user.

Many organizations use CDNs to cache website content to meet their performance and security needs. The demand for CDN services is increasing as websites offer more streaming video, e-commerce and cloud applications, where high performance is key. Few CDNs have POPs in every country. As a result, organizations must use several CDN providers to ensure they meet the needs of their customers and users, wherever they are located.

Besides content caching and web delivery, CDN providers offer services that complement their core functionality and capitalize on their presence at the network edge. These include security services for distributed denial-of-service (DDoS) Protection, web application firewalls (WAFs) And bot mitigation.

REFERENCES

https://www.techtarget.com/searchnetworking/definition/CDN-content-delivery-network

https://www.cdnetworks.com/what-is-a-cdn/

FOG COMPUTING

ANANYA G S(21MCA03)

SMRUTHI R(21MCA40)

Fog computing, also called edge computing, is intended for distributed computing where numerous "peripheral" devices connect to a cloud. The word "fog" refers to its cloud-like properties, but closer to the "ground", i.e., IoT devices. Many of these devices will generate voluminous raw data (e.g., from sensors), and rather than forward all this data to cloud-based servers to be processed, the idea behind fog computing is to do as much processing as possible using computing units co-located with the data-generating devices, so that processed rather than raw data is forwarded, and bandwidth requirements are reduced. An additional benefit is that the processed data is most likely to be needed by the same devices that generated the data, so that by processing locally rather than remotely, the latency between input and response is minimized. This idea is not entirely new: in non-cloud-computing scenarios, special-purpose hardware (e.g., signal-processing chips performing Fast Fourier Transforms) has long been used to reduce latency and reduce the burden on a CPU.

Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives (e.g. operational costs, security policies, resource exploitation), dense geographical distribution and context-awareness (for what concerns computational and IoT resources), latency reduction and backbone bandwidth savings to achieve better quality of service(QoS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure while it is also able to be used in Assisted Living scenarios.

Fog networking supports the Internet of Things (IoT) concept, in which most of the devices used by humans on a daily basis will be connected to each other. Examples include phones, wearable health monitoring devices, connected vehicle and augmented reality using devices such as the Google Glass. IoT devices are often resource-constrained and have limited computational abilities to perform cryptography computations. A fog node can provide security for IoT devices by performing these cryptographic computations instead.

SPAWAR, a division of the US Navy, is prototyping and testing a scalable, secure Disruption Tolerant Mesh Network to protect strategic military assets, both stationary and mobile. Machine-control applications, running on the mesh nodes, "take over", when Internet connectivity is lost. Use cases include Internet of Things e.g., smart drone swarms.

ISO/IEC 20248 provides a method whereby the data of objects identified by edge computing using Automated Identification Data Carriers (AIDC), a barcode and/or RFID tag, can be read, interpreted, verified and made available into the "Fog" and on the "Edge," even when the AIDC has moved on.

REFERENCES:

Fog computing - Wikipedia

SECURITY MECHANISM

ANDRIYA DSOUZA (21MCA04)

PRIYADARSHNI N(21MCA31)

Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore, security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.

Types of Security Mechanism are

1. **ENCIPHERMENT**
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

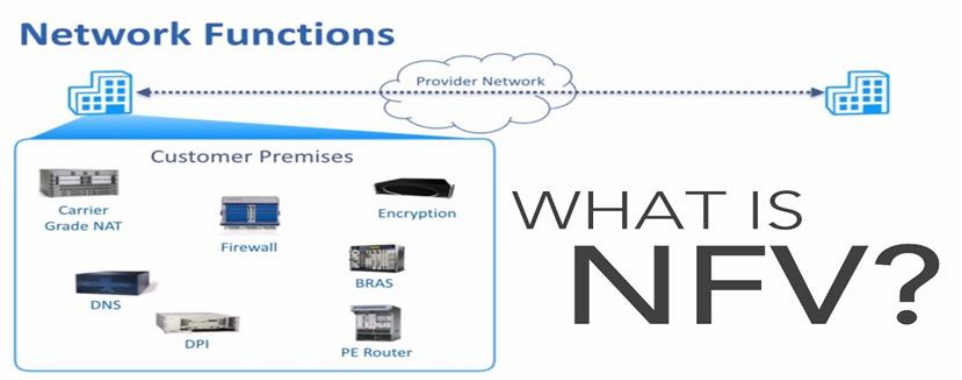
2. **ACCESSCONTROL**
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
3. **NOTARIZATION**
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
4. **DATAINTEGRITY**
   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
5. **AUTHENTICATIONEXCHANGE**
   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
6. **BITSTUFFING**
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
7. **DIGITALSIGNATURE**
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

NETWORK FUNCTIONS VIRTUALIZATION

HARI PRIYA S(21MCA)

RABIYA BASRI (21MCA)

Network functions virtualization (NFV) is a network architecture concept that leverages the IT virtualization technologies to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create and deliver communication services.



WHAT IS NFV:

Network functions virtualization (NFV) is the replacement of network appliance hardware with virtual machines. The virtual machines use a hypervisor to run networking software and processes such as routing and load balancing.

NETWORK FUNCTIONS THAT CAN BE VIRTUALIZED WITH NFV INCLUDES:

- Domain Name Service (DNS),
- Network Address Translation (NAT)
- firewalls, and caching.

THE BENEFITS OF NETWORK FUNCTION VIRTUALIZATION IS:

- Reduced space needed for network hardware.
- Reduce network power consumption.
- Reduced network maintenance costs.
- Easier network upgrades.
- Longer life cycles for network hardware.
- Reduced maintenance and hardware costs.

REFERENCES:

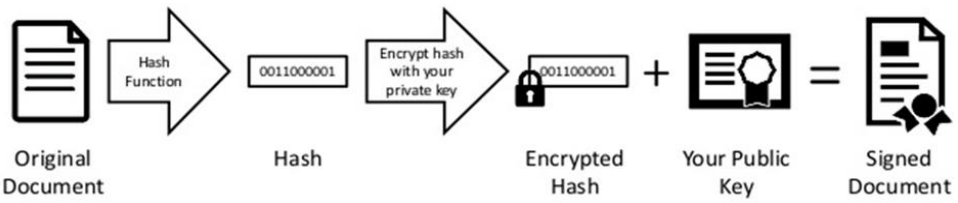
https://www.blueplanet.com/resources/What-is-NFV-prx.html

https://www.vmware.com/topics/glossary/content/network-functions-virtualization-nfv.html

DIGITAL SIGNATURE

LAKSHMI SHRUTI J(21MCA23)

ASHRITA G(21MCA06)



A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key. If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated. Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder. To create a digital signature, signing software, such as an email program, is used to provide a one-way hash of the electronic data to be signed. A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature.

References :

www.techtarget.com

www.tutorialspoint.com

TRANSMISSION MEDIA IN COMPUTER NETWORK

VIDYA.M(21MCA)

DIVYA SHREE.K(21MCA)

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

Some factors need to be considered for designing the transmission media:

- Bandwidth: All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- Transmission impairment: When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- Interference: An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Classification Of Transmission Media:

1. Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath.

(ii) Coaxial Cable –
It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.

(iii) Optical Fiber Cable –
It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding.

2. Unguided Media:
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

- Radio waves
- Micro waves
- Infrared

TRAFFIC ENGINEERING IN SOFTWARE DENIED NETWORKS

CH. CHANDANA (21MCA10)

STEFFI.P (21MCA4)

INTRODUCTION

A major problem with underlying communication network is the dynamic nature of the network applications and their environment. This means that the performance requirements of the transferred data flows, like Quality of Service (Q o S), can vary over time. The applications operate in a wide range of environments, i.e., wired and wireless with a variety of networking devices. For the applications to perform effectively, the underlying network should be flexible enough to dynamically change in response to any changes in the application requirements and their environment. The current approaches are either based on static or over provisioned overlay networks, or require the applications to change in accordance with the network performance. An important way to address this problem is through traffic engineering (TE). It is the process of analyzing the network state, predicting and balancing the transmitted data load over the network resources.

ABSTRACT

An important technique to optimize a network and improve network robustness is traffic engineering. As traffic demand increases, traffic engineering can reduce service degradation and failure in the network. To allow a network to adapt to changes in the traffic pattern, the research community proposed several traffic engineering techniques for the traditional networking architecture. However, the traditional network architecture is difficult to manage. Software Defined Networking (SDN) is a new networking model, which decouples the control plane and data plane of the networking devices. It promises to simplify network management, introduces network programmability, and provides a global view of network state.

Software-Defined Networking (SDN)

With the continuous development and in-depth application of cloud computing and Internet of Things (IoT) , the traditional network architecture cannot meet the requirements of current industry fields, such as Cyber-Physical Systems(CPS) , 5G wireless network , and Internet of Vehicle . Therefore, some researchers proposed that Software Defined Network (SDN) will be applied to the industrial environment, which will increase flexibility and innovation capacity of IoT in industrial system .

Security and Traffic Engineering (TE) are both research topics for SDN applications in the fields of industrial environments. In the literature , we studied security issues of SDN, in this paper, we will mainly focus on the TE problem of SDN. TE is an important application related to network systems, whose main task is to study how to measure and analyze real-time network traffic, and design reasonable routing mechanisms to schedule and guide network traffic to improve utilization of network resources, or better meet requirements of the network Quality of Service (QoS).

CHARACTERISTICS:

- Concentration of control
- Programmability
- Openness
- Traffic measurement
- Traffic scheduling and management

FRAMEWORK FOR TE IN SDN

Combining the ideas of TE for traditional networks with characteristics of the SDN, we propose a framework for TE in the SDN, as illustrate

REFRENCES:

- W. Xia, Y. Wen, C. H. Foh, D. Niyato, H. Xie, A survey on software-defined networking, IEEE Communications Surveys & Tutorials 17 (1) (2015) 27–51.
- H. Farhady, H. Lee, A. Nakao, Software-defined networking: A survey, Computer 455 Networks 81 (2015) 79–95.

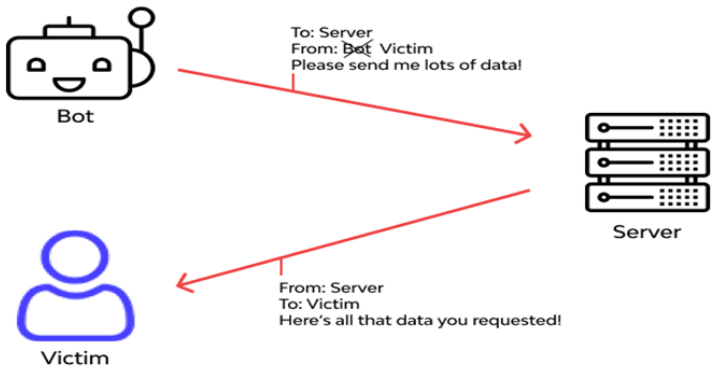
IP SPOOFING

S PAVITHRA (21MCA37)

PADMA PRIYA (21MCA27)

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.

It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.



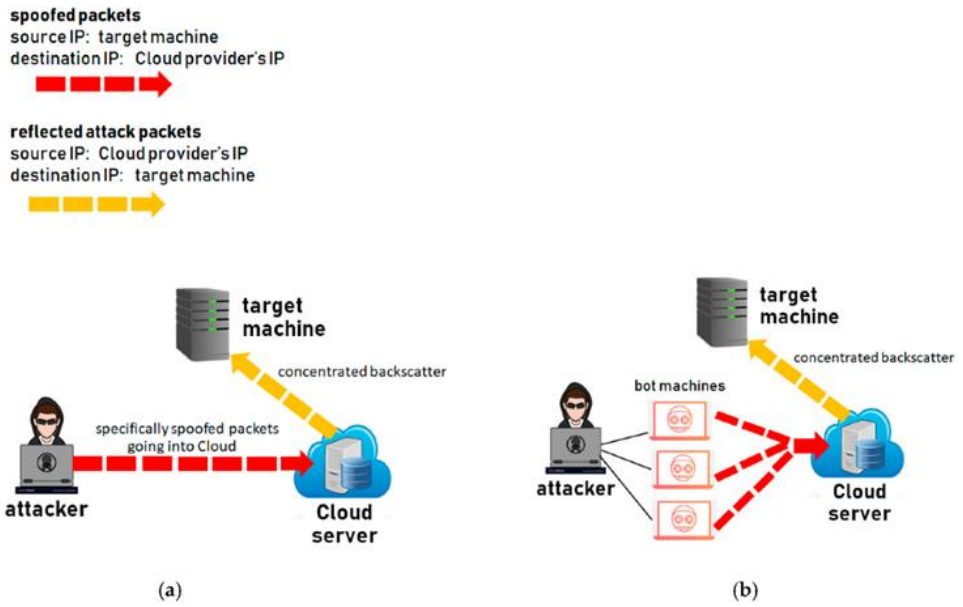
TYPES OF IP SPOOFING

- IP spoofing: attacker uses IP address of another computer to acquire information or gain access from another network.
- E-mail spoofing: attacker sends e mail but makes it appear to come from someone else (reliable e-mail).
- Web spoofing: attacker tricks web browser into communicating with a different web server than the uses intended.

TYPES OF IP SPOOFING ATTACKS

The IP spoofing can further cause various attacks. These attacks can be caused by the IP spoofing.

1) Blind Spoofing
2) Denial-of-service attack
3) Man-in-the-middle attack



APPLICATION

- IP address spoofing involving the use of a trusted IP address
- This type of attack is most effective where trust relationships exist between machines.
- By spoofing a connection from a trusted machine, an attacker on the same network may be able to access the target machine without authentication.

ADVANTAGES

- Allows for detailed distribution pf packets.
- Bottle necks.

DISADVANTAGES

- Need to work with raw sockets and alter packets. Very complicated.
- Single point of failure.

CONCLUSION

- IP-Spoofing is an exploitation of trust-based relationship and can be curbed effectively if proper measures are used.
- Understanding how and why spoofing attacks are used , combined with a few simple prevention methods, can help protect networks from these malicious cloaking and cracking techniques.

REFERENCE

- https://www.iplocation.net/ip-spoofing
- https://en.wikipedia.org/wiki/IP_address_spoofing

SDN (SOFTWARE DEFINED NETWORKING)

POOJA (21MCA28)

NIVEDITA (21MCA26)

Software-Defined Networking (SDN) The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.

SDN ARCHITECTURE:

DIRECTLY PROGRAMABLE:

Network control is directly programmable because it is decoupled from forwarding functions.

AGILE:

Network control is directly programmable because it is decoupled from forwarding function.

CENTRALLY MANAGED:

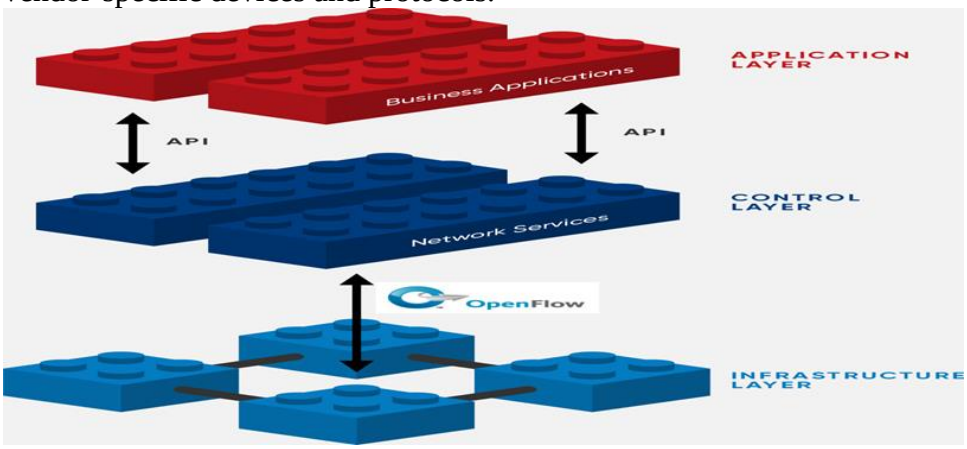
Networking intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch

PROGRAMMATICALLY CONFIGURED:

SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the program do not depend on proprietary software.

OPEN STANDARDS-BASED AND VENDOR-NEUTRAL:

When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.



REFRENCE

https://opennetworking.org/sdn-definition/