



Vol. 6

TECHNO MUTATION

2020

Technique Polytechnic Institute
Panchrokhi, Sugandhya, Hooghly



Department of
Computer Science & Technology
NBA Accredited



contact : (033) 2686-3682(exl:t:216)
email : dcst@techniqueedu.com



institutional

Vision

To make Technique Polytechnic Institute a CENTRE OF EXCELLENCE in learning, teaching and knowledge transfer in an ambience of Humanity, Wisdom, Intellect, Knowledge, Creativity and Innovation in order to nurture our students to become culturally and ethically rich professionals with bright future of our country.

Mission

institutional

To provide Knowledge with Academic Excellence and to prepare our students for their successful professional career.

To inspire our Faculty members to always Excel and in turn Motivate the Students to achieve Excellence.

To provide a stimulating learning environment with a technological orientation to maximize individual Potential.

To develop innovative and efficient use of modern instructional technology.

To ensure our students of all ability levels are well equipped to meet the challenges of education, work and life.

To encourage development of interdisciplinary research, which addresses strategic needs of industry and society.

To encourage and support professional development for faculty and staff.

To educate and prepare students to contribute as engineers and citizens through the creation, integration, application, and transfer of engineering knowledge





Departmental **Vision:**

To be a dynamic and efficient department of Computer Science & Technology providing quality education and progressive atmosphere to the students so that they can implement knowledge effectively to meet the needs of society

Departmental **Mission:**

- 1) To Provide a learning ambience to enhance innovations, problem solving skills, leadership qualities, team-spirit and ethical responsibilities.*
- 2) To Provide exposure to latest tools and technologies in the area of engineering and technology*
- 3) To motivate student to pursue higher studies will always be alive.*
- 4) To Support society by participating in and encouraging technology transfer.*



Index

Message from editorial team

Dynamic Approach for the Isolation of Version Number Attack in IoT based on Threshold Value

ZigBee Wireless Technology Architecture and Applications

Wireless AI

The age of Virtual Reality, Augmented Reality and Mixed Reality

Rooting Android

Cryptography

Ethical Hacking

Digital Image Processing (DIP)

Robotic Process Automation (RPA)

Artificial Intelligence - Myth Vs Fact

3-D Home Printers Could Change Economy

Cyber Security - "A Boon To The Digitally Emerging Era"

WiMAX



Message from editorial team

It gives us immense pleasure and satisfaction to re-introduce our departmental technical magazine "technomutation vol-3" for the session 2017-18. A lot of effort has gone into the making of this issue. We hope you enjoy reading the magazine. The best thing about this issue is that it represents the contemporary face of DCEI students. Amidst the busy schedule of a 4-month semester, with 3-exams, surprise quizzes and all those assignments and problem sheets that make you want to bang your head on the wall, it is fascinating to see how students are keeping abreast with trending technologies. So this time we have made an attempt to bring out the talent concealed within our student community. Faculties of the department has also contributed from their end by touring the grayer side of technical issues. This volume indulges research in one hand on other it presents cutting edges technologies. We hope you enjoy reading this issue as much as we have enjoyed making it.



Editor in Chief
Sudeshna Sani

Co-Editor
Sohan Goswami

Members:
Debasish Hati
Soumali Roy
Shildas Bhattacharya

Dynamic Approach for the Isolation of Version Number Attack in IoT based on Threshold Value

Debasish Hati
Lecturer, DCST

ABSTRACT

The internet of things is the self configuring type of network in which various nodes can join or leave the network when they want. Due to such nature of the network, various malicious nodes can join or leave the network. The version number attack is the active type of attack which affects network performance. In this research work, technique of threshold is proposed for the detection and isolation of malicious nodes from the network. The proposed technique is implemented in network simulator version 2 and results are analyzed in terms of packet loss, delay and throughput.

Keywords

Version number attack, DODAG, Threshold Technique

1. INTRODUCTION

IoT (Internet of Things) can be defined as a technology that connects multiple sensors, smart nodes, and objects together for establishing communication among them without any manual intervention. The autonomous functioning of entities or things depends on the connectivity amid them. The nodes in IoT carry out different types of tasks. These tasks include analysis of gathered data for decision making, giving lightweight data and data extraction by getting the excess of the cloud-based resources. The connection between clients, services, sensors and objects is established extremely closely via IoT. There are various application fields that make use of IoTs in extensive manner. These application fields include smart grid healthcare, ITS (Intelligent Support System). IoT is highly beneficial from business prospective also as it provides large number of intelligent tools and services [1]. The connectedness of IoT devices on the cloud system is the main reason behind

the development of cloud-based IoT networks. This makes possible the transmission of data to serve different purposes. In particular, IP based web and IoT applications provide transferring using TCP and UDP. On the other hand, few commonly used message distribution functions occur amongst the majority of IoT applications. Different applications apply these tasks in interoperable standard manners. The designing of a publish/subscribe protocol framework, extremely analogous to the client/server protocol, is carried out. This is referred as MQTT (Message Queue Telemetry Transport). MQTT protocol becomes highly important because of its uncomplicated structure and capability to prevent the extreme use of CPU and memory. AMQP (Advanced Message Queuing Protocol) is the one more protocol developed for the financial industry. The main motive behind using TLS/SSL protocols is security management. The use of less power and memory embedded devices can be ensured by using CoAP for the communication purpose.

Up to now, several network layer protocols have been designed as well. Among these protocols, IEEE 802.15.4 is the most frequently used IoT standard for MAC protocol [7]. This protocol defines a frame set-up. In this set-up, the address of source and destination is defined in headers along with way through which node can interact with each other. In recent times, the implementation of Low power multi-hop networking is carried out in IoT due to its unsuitability of using frame formats implemented earlier in the conventional networks. They increase the system's overhead. In general, channel hopping and time synchronization are employed to ensure high consistency, inexpensiveness and to satisfy the communication requirements of

internet of things. The IPv6 Routing Protocol is a standardized remote vector routing protocol. This protocol is specially designed for RPL network which is lossy and includes low energy. This protocol does not include any cycle, and therefore does not have loop. This occurs due to the way in devices are linked to each other. DODAG with the border routers avoids cycles. These routers are linked to the internet. All devices linked to DODAG are connected online via this border router. The protocol prevents

1.1 Version Number Attack

The root node makes use of version number to ensure that the global repair process of RPL is under control and updating of all the nodes existing in DODAG is carried out based on their routing location. The occurrence of version number attacks in IoT can decrease its service time. The intruder can launch this intrusion with extremely low overhead and the use of global repair scheme included as an immune system of protocol can overload the global repair scheme network. The root starts a global repair in the occurrence of numerous network irregularities [14]. The VN (Version Number) of DODAG is incremented to rebuild the entire DODAG. DIO (DODAG Information Object) refers to the control message that carries this version number. Every receiving node compares the earlier version number and the one obtained from its parent. The existing rank information is overlooked, the trickle timers are reset and a novel process to join the DODAG is started in case of higher received version. This global repair guarantees a loop free topology despite of its too much expensiveness. It is important to notice that the node did not transit to the novel DODAG version if DIO messages advertize its earlier version. It is essential for the other nodes to not choose such a node as preferred parent. Two versions of DODAG may occur simultaneously during global repair. On the other hand, data packets existing in old version can migrate in fresh version to prevent loops. The earlier version is not regarded as DODAG. Also, the accessibility

loops when it measures the location of node corresponding to the root node [9]. This position regarding the root node is referred as the rank and the rank increases with the motion away from the border router. Messages from a child node which is going down are ignored to prevent loops. A node contains a parent, which transfers data from the nodes to the border router and may have various children. The node sends the children's packages to the border router.

of loop free topologies cannot be guaranteed as the network is still away from the convergence state.

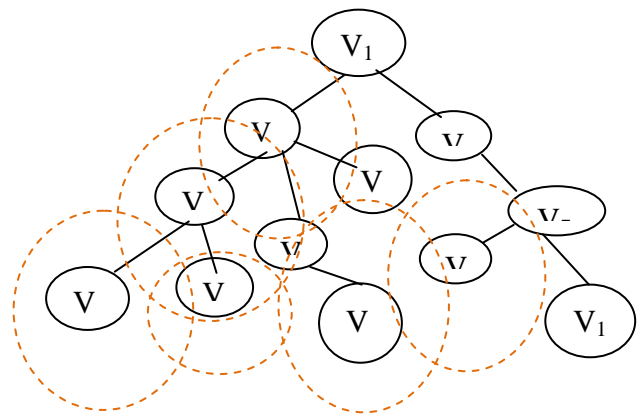


Figure 1 Illustration of a version number attack [14]

In order to prevent any possible irregularities of the network, the version number must be transmitted unaltered across DODAG. RPL does not include any method to ensure the reliability of version number occurring in the received DIO messages. An attempt made by the malicious node to change this value in its own DIO messages can cause harm to the network. If a malevolent DIO is received with a fresh version number, the trickle timer is reset, the version is updated and the fresh version is promoted to the neighbors by DIO messages. Figure 1.4 shows the propagation of the illegal version number via the network. In this situation, the genuine network nodes broadcast their increased version number started by malevolent node V_5 in the automatic manner.

2. LITERATURE REVIEW

Ahmet Ariset *al.*[16], presented two new lightweight mitigation schemes for RPL-VNA (Version Number Attacks). These intrusions severely affected the efficiency of IPv6-connected LLNs (Low Power and Lossy Networks). In these intrusions, an intruder cause changes in the version number of the network spitefully. The main aim of the attacker here was to increase the latency and control message overhead. These types of intrusions reduced the service time of network and PDR (Packet Delivery Ratio). This work presented simple at the same time efficient mitigation methods to significantly improve the efficiency of attack affected RPL network. The new schemes reduced the attack caused delay, average power consumption and control message overhead up to 87%, 63%, and 71%. These schemes also showed 86% of increase in the PDR (Packets Delivery Ratio). The new schemes exchanged the mitigation efficiency against the resource outlays while permitting the ordinary RPL function. Hence, these schemes allowed network manager to select the appropriate technique for their RPL network

Amit Dvir *et al.* [17], presented a novel routing protocol to remove the problems of LLNs (Low power and Lossy networks). This protocol was referred as IPv6 routing protocol. The new protocol made its contribution in the performance of LLNs (Low power and Lossy Networks). RPL provided multiple routes by generating and handling the DAGs (Directed Acyclic Graphs) via single or multiple gateways. Therefore, an adversary deploying a single node close to the gateway could divert a bigger part of the network traffic independently. This work made use of an improve version called DODAG to reconstruct the routing topology. It was also essential to carefully prevent an internal attacker from publishing the reduced rank level that caused a bigger portion of the DODAG for establishing connection to the DODAG root through the intruder and made it

enable to listen to a bigger portion of the network traffic forward on its own. Hence, this new security approach was capable enough to prevent the illegal boost in the version number.

Anthea Mayzaudet *al.* [18], proposed a detection technique derived from a distributed monitoring framework with dedicated algorithms. The main aim of this technique was to detect VNAs (version number attacks) in RPL-based networks using a distributed monitoring framework. The new technique successful identified the malevolent nodes that launched these types of intrusions in RPL networks. A lot of tests were conducted in this work to evaluate the efficiency of the proposed technique. This work considered a monitoring node placement scheme to quantify the scalability of the new technique. The future work would be focused on conducting corresponding tests in real-time architectures with more types of devices applying the RPL protocol. In future, the proposed technique could be evaluated and extended to the case of intruder alliance. It refers to the condition when various adversary nodes occur in the network simultaneously.

Zeeshan Ali Khan *et al.* [19], designed and evaluated some IDS schemes for IoT Networks. These schemes were suitable for the minute devices. These schemes made use of trust management method. This method allowed devices to handle reputation information of their neighbors. This approach efficiently distinguished spitefully behaving elements in a processing and energy-efficient manner. This procedure was carried out in an energy based system. The trust management subjective logic was focused on to recognize the adversary nodes existing in the network. Three variables were presented. These variables were based on negative and positive trust ratings; belief (b), disbelief (d) and uncertainty (u)

$$b = \frac{p}{p + n + k} \quad d = \frac{n}{p + n + k} \quad u = \frac{k}{p + n + k}$$

The adversary node after being detected got immediately eliminated from the network. The new scheme performed better against the three sorts of intrusions launched on RPL protocol. It was possible to use the new scheme against the other sorts of attacks as well. The future work would be focused on developing a test bed containing Z1 elements to validate the simulation results of MATLAB tool. This work made a discussion on a variety of algorithms to manage the reputation. These algorithms included NBTD (Neighbor Based Trust Dissemination), CNTD (Clustered Neighbor Based Trust Dissemination) and TTD (Tree Based Trust Dissemination).

H. Abdoet *et al.* [20], presented a new technique based on both safety as well security during for analyzing the risk in industrial applications. This technique combined bowtie analysis with a fresh improved adaptation of attack tree analysis. The use of bowtie analysis was quite popular to analyze the security while the second approach was presented to analyze the safety of ICS (Industrial Control Systems). The bowtie and attack tree when merged together comprehensively represented the risk conditions by considering safety and security. Afterward, this work presented a technique to evaluate the risk level on the basis of two-folded possibility portions. The first portion was used for the safety while the other one was for the security. This work analyzed a real-time risk case in a chemical factory to represent the purpose of this technique.

Ahmet Aris *et al.* [21], deeply studied the RPL version number attacks and presented the analysis of intrusions from different viewpoints. This analysis gave exclusive factors of this work in a real-time network topology. This topology had both stationary and mobile nodes with different multiplicities. This work was inspired from the IETF routing requirement documents. This work also analyzed the way of affecting the energy consumption of the nodes by the VNA (Version Number Attack). This work presented a probabilistic attacking model. In

this model, the intruder launched intrusion attacks with a probability of p (e.g., 0, 0.3, 0.5, 0.7, and 1). This work also provided the performance outcomes in terms of different values of probability of p . The simulation results demonstrated that the outcomes of PDR (Packet Delivery Ratio) and the CPO (Control Packet Overhead) were highly related to the intruder's locality.

Hezam Akram Abdul-Ghani *et al.* [22], presented a novel IoT (Internet of Things) suggestion approach based on the construction of blocks strategy. This was mainly a reference model with four layers. This work presented a wide-ranging IT attack model that had four major stages. The first stage presented an IoT asset based attack level made up of four elements. These elements were identified as software, information, protocol wrapping the complete IoT mass and significant things. The next stage provided a description of the IoT security architecture. The third stage classified the IoT attack for all elements. The last stage detected the infringement of security objectives and relation between each intrusion. This stage also presented various strategies to secure every resource. This was the first ever attempt of developing an IoT attack model based on the building block reference model. The achieved outcomes evidently demonstrated the efficiency of the new model.

Anthea Mayzaud *et al.* [23], presented a detection approach to deal with the VNA (Version Number Attack) in RPL environment. This work applied a strategy relied on the distributed monitoring architecture to hold a discussion on node resources. The new approach used the relationship amid monitored nodes for the intruder detection. The intruder started the localization process after getting the detection information from all observing nodes. In this work, several tests had been carried out to evaluate the new approach. It was possible to decrease the FPR (False Positive Rate) by placing the monitoring nodes strategically. The future work would be focused

on conducting a large number of corresponding tests on the basis of realistic framework with some other types of devices.

3. RESEARCH METHODOLOGY

There are several stages included in the research method. These stages include implementation strategy, projected results and requirements for hardware and software tools.

Here are the different steps of the implementation strategy:-

- **Deployment of the Network:** - The deployment of network will be carried out with the fixed number of sensor nodes and a sink node. The sensor nodes sense different sorts of physical parameters such as temperature, pressure etc. The sensor devices are heterogeneous in nature. This implies that every sensor node possesses different battery and processing energy. The DODAG protocol will sort out the network into a configuration similar to the tree.
- **Trigger of version number attack:** - The malevolent nodes will be formed in the network. These nodes launch version number intrusion. In the DODAG, malicious nodes cause changes in the version number. The DODAG protocol will choose the route with high version number. This will result in routes based on loop formation in IoT.
- **Trust Calculation:** - This work presents trust based approach to mitigate the version number intrusion. The trust based scheme will perform in the three stages. These stages include pre-processing, trust measurement and trust updating. The sensor nodes with minimum trust will be marked as malevolent nodes.
- **Analyze network performance:** - The final stage will analyze the efficiency of network in terms of some metrics. These metrics include throughput, packet loss and energy consumption. The efficiency of the new method is evaluated using this metrics.

4. RESULT AND DISCUSSION

This research work is focused on to isolate version number attack in IoT. The version number attack is launched in the DODAG protocol. This chapter compares the three conditions. The first two conditions include DODAG protocol and the effect of version number attack on the efficiency of DODAG protocol with regard to throughput and packet loss. The third case involves the segregation of version number intrusion in DODAG protocol. As per the analysis, the presented case has minimum packet loss and maximal number of throughput in contrast to attack case presented in the base paper.

Table 1: Simulation Parameters

Parameter	Values
Simulator	Ns2-2.35
Number of nodes	32
Area	800 * 800 meter
Antenna type	Omi-directional
Channel	Wireless channel
Propagation Model	Two ray

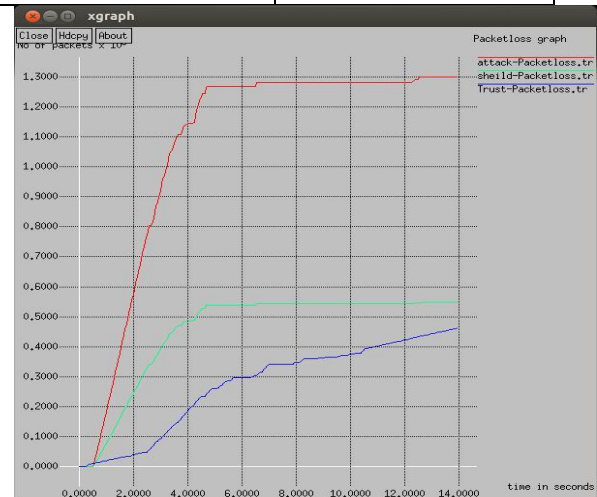


Fig 1: Analysis of packet loss

Figure 1 shows the comparison of attack case, base paper case and proposed case in terms of packet loss. As per the analysis, the presented

technique shows minimal number of packet loss in contrast to the other two cases.



Fig 2: Throughput Comparisons

Figure 2 shows the comparison of attack case, base paper case and proposed case in terms of throughput. As per the analysis, the presented technique shows maximal throughput in contrast to the other two cases.



Fig 3 Delay Comparison

Figure 3 shows the comparison of attack case, shield attack and proposed approach in terms of delay. Shield scenario refers to the earlier technique for isolating the version number intrusion. As per the analysis, the presented technique shows minimal delay in contrast to the other two cases.

5. CONCLUSION

This work is focused on to mitigate the version number attack in IoT. DODAG is a hierarchical structure. RPL network makes use of this structure for tiny devices where the malevolent nodes increments the version number. In IoT, this results in the formation of path containing loop. This work presents trust based approach to mitigate the version number intrusion from the network, and detecting the malevolent nodes. This approach consumes minimum number of IoT resources. This work makes use of NS2 (network simulator version 2) to implement the presented approach. The analysis of outcomes has been carried out in terms of throughput and packet loss. As per the analysis, the new approach performs better than other two cases in terms of throughput. The packet loss of the presented case is lower than the other two cases.

References

- [1] A. Shaddad Abdul-Qawy, P. Pramod, E. Magesh, and T. Srinivasulu, "The Internet of Things (IoT): An Overview," *J. Eng. Res. Appl.*, vol. 5, no. 12, pp. 71–82, 2015.
- [2] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wirel. Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011.
- [3] V. Bhuvaneswari and R. Porkodi, "The internet of things (IoT) applications and communication enabling technology standards: An overview," *Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014*, pp. 324–329, 2014.
- [4] S. V. Pote, "Internet of Things Applications , Challenges and New Technologies," vol. 67, no. 978, pp. 45–51, 2018.
- [5] E. Hopalı and Ö. Vayvay, "Internet of Things (IoT) and its Challenges for Usability in Developing Countries," vol. 2, no. January, pp. 6–9, 2018.
- [6] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review,"

Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.

[7] T. Salman and R. Jain, “Networking protocols and standards for internet of things,” *Internet Things Data Anal. Handb.*, vol. 1, no. 1, pp. 215–238, 2017.

[8] Aniruddha Chakrabarti, “Emerging Open and Standard Protocol Stack for IoT | Aniruddha Chakrabarti | Pulse | LinkedIn,” vol. 1, no. 1, pp. 2–6, 2015.

[9] Internet Engineering Task Force. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. <https://tools.ietf.org/pdf/rfc6550.pdf>, 2012. [Online; accessed 02-June 2017].

[10] E. Baccelli, M. Philipp, and M. Goyal, “The P2P-RPL Routing Protocol for Ipv6 Sensor Networks: Testbed Experiments,” *SoftCOM 2011, 19th Int. Conf. Software, Telecommun. Comput. Networks, Split*, vol. 1, pp. 1–6, 2011.

[11] T. Zhang and X. Li, “Evaluating and analyzing the performance of RPL in contiki,” *Proc. first Int. Work. Mob. sensing, Comput. Commun. - MSCC '14*, pp. 19–24, 2014.

[12] J. Posegga, T. Eder, D. Nachtmann, D. Parra, and D. Schreckling, “Conference Seminar SS2013 — Real Life Security (5827HS) Trust and Reputation in the Internet of Things Trust and Reputation in the Internet of Things,” pp. 1–19, 2013.

[13] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, “A Trust-based Resilient

Routing Mechanism for the Internet of Things,” *Proc. 12th Int. Conf. Availability, Reliab. Secur. - ARES '17*, pp. 1–6, 2017.

[14] A. Mayzaud, R. Badonnel, and I. Chrisment, “A distributed monitoring strategy for detecting version number attacks in RPL-based networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 14, no. 2, pp. 472–486, 2017.

[15] J. Guo, I. R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” *Comput. Commun.*, vol. 97, pp. 1–14, 2017.

[16] A. Arış, S. B. Örs Yalçın, and S. F. Oktuğ, “New lightweight mitigation techniques for RPL version number attacks,” *Ad Hoc Networks*, vol. 85, pp. 81–91, 2019.

[17] A. Dvir, T. Holczer, and L. Buttyan, “VeRA - Version number and rank authentication in RPL,” *Proc. - 8th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst. MASS 2011*, pp. 709–714, 2011.

[18] A. Mayzaud, R. Badonnel, and I. Chrisment, “Detecting version number attacks in RPL-based networks using a distributed monitoring architecture,” *2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016*, pp. 127–135, 2017.

In this present communication world there are numerous high data rate communication standards that are available, but none of these meet the sensors' and control devices' communication standards. These high-data rate communication standards require low-latency and low-energy consumption even at lower bandwidths. The available proprietary wireless systems' Zigbee technology is low-cost and low-power consumption and its excellent and superb characteristics makes this communication best suited for several embedded applications, industrial control, and home automation, and so on.

What is Zigbee Technology?

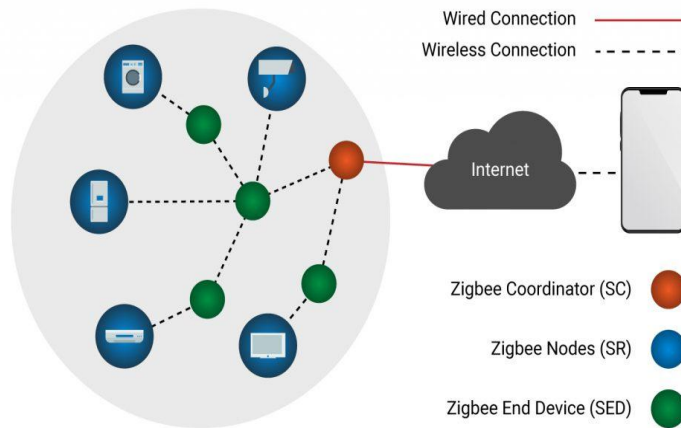
Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz and 2.4 GHz frequencies. The data rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.



Zigbee supports different network configurations for master to master or master to slave communications. And also, it can be operated in different modes as a result the battery power is conserved. Zigbee networks are extendable with the use of routers and allow many nodes to interconnect with each other for building a wider area network.

Zigbee Architecture

Zigbee system structure consists of three different types of devices such as Zigbee coordinator, Router and End device. Every Zigbee network must consist of at least one coordinator which acts as a root and bridge of the network. The coordinator is responsible for handling and storing the information while performing receiving and transmitting data operations. Zigbee routers act as intermediary devices that permit data to pass to and fro through them to other devices. End devices have limited functionality to communicate with the parent nodes such that the battery power is saved as shown in the figure. The number of routers, coordinators and end devices depends on the type of network such as star, tree and mesh networks.

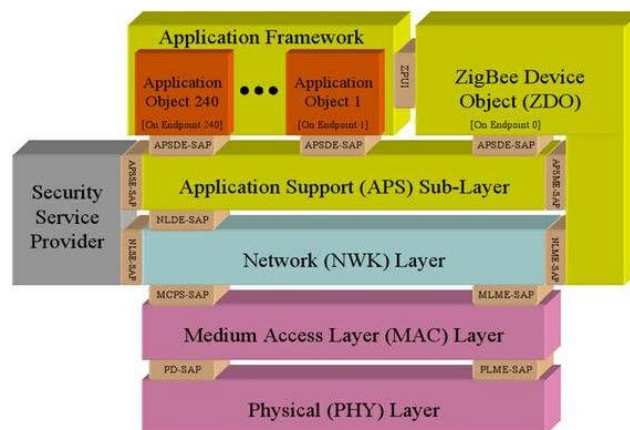


Zigbee Protocol Architecture

Physical Layer: This layer does modulation and demodulation operations up on transmitting and receiving signals respectively.

MAC Layer: This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance (CSMA). This also transmits the beacon frames for synchronizing communication.

Network Layer: This layer takes care of all network related operations such as network setup, end device connection and disconnection to network, routing, device configurations, etc.



Application Support Sub-Layer: This layer enables the services necessary for Zigbee device object and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

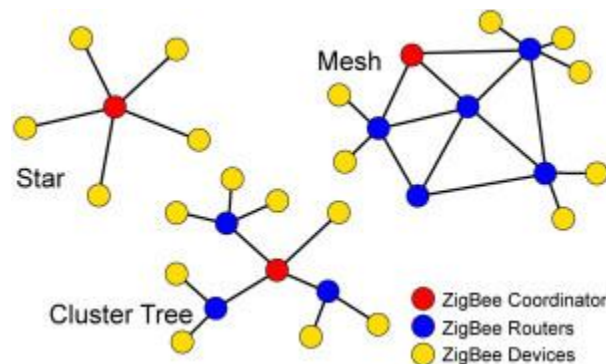
Application Framework: It provides two types of data services as key value pair and generic message services. Generic message is a developer defined structure, whereas the key value pair is used for getting attributes within the application objects. ZDO provides an interface between application objects and APS layer in Zigbee devices. It is responsible for detecting, initiating and binding other devices to the network.

Zigbee Operating Modes and Its Topologies

Zigbee two way data is transferred in two modes: Non-beacon mode and Beacon mode. In a beacon mode, the coordinators and routers continuously monitor active state of incoming data hence more power is consumed. In this mode, the routers and coordinators do not sleep because at any time any node can wake up and communicate. However, it requires more power supply and its overall power consumption is low because most of the devices are in an inactive state for over long periods in the network.

In a beacon mode, when there is no data communication from end devices, then the routers and coordinators enter into sleep state. Periodically this coordinator wakes up and transmits the beacons to the routers in the network. These beacon networks are work for time slots which means, they operate when the communication needed results in lower duty cycles and longer battery usage. These beacon and non-beacon modes of Zigbee can manage periodic (sensors data), intermittent (Light switches) and repetitive data types.

Zigbee Topologies



Zigbee supports several network topologies; however, the most commonly used configurations are star, mesh and cluster tree topologies. Any topology consists of one or more coordinator. In a star topology, the network consists of one coordinator which is responsible for initiating and managing the devices over the network. All other devices are called end devices that directly communicate with coordinator. This is used in industries where all the end point devices are needed to communicate with the central controller, and this topology is simple and easy to deploy.

In mesh and tree topologies, the Zigbee network is extended with several routers where coordinator is responsible for starting them. These structures allow any device to communicate with any other adjacent node for providing redundancy to the data. If any node fails, the information is routed automatically to

other device by these topologies. As the redundancy is the main factor in industries, hence mesh topology is mostly used. In a cluster-tree network, each cluster consists of a coordinator with leaf nodes, and these coordinators are connected to parent coordinator which initiates the entire network.

Due to the advantages of Zigbee technology like low cost and low power operating modes and its topologies, this short range communication technology is best suited for several applications compared to other proprietary communications, such as Bluetooth, Wi-Fi, etc.

Applications of Zigbee Technology

Industrial Automation: In manufacturing and production industries, a communication link continually monitors various parameters and critical equipments. Hence Zigbee considerably reduce this communication cost as well as optimizes the control process for greater reliability.

Home Automation: Zigbee is perfectly suited for controlling home appliances remotely as a lighting system control, appliance control, heating and cooling system control, safety equipment operations and control, surveillance, and so on.

Smart Metering: Zigbee remote operations in smart metering include energy consumption response, pricing support, security over power theft, etc.

Smart Grid monitoring: Zigbee operations in this smart grid involve remote temperature monitoring, fault locating, reactive power management, and so on.

How AI is Starting to Influence Wireless Communications

Machine learning and deep learning technologies are promising an end-to-end optimization of wireless networks while they commoditize PHY and signal-processing designs and help overcome RF complexities

What happens when artificial intelligence (AI) technology arrives on wireless channels? For a start, AI promises to address the design complexity of radio frequency (RF) systems by employing powerful machine learning algorithms and significantly improving RF parameters such as channel bandwidth, antenna sensitivity and spectrum monitoring.

So far, engineering efforts have been made for smartening individual components in wireless networks via technologies like cognitive radio. However, these piecemeal optimizations targeted at applications such as spectrum monitoring have been labor intensive, and they entail efforts to hand-engineer feature extraction and selection that often take months to design and deploy.

On the other hand, AI manifestations like **machine learning** and **deep learning** can invoke data analysis to train radio signal types in a few hours. For instance, a trained deep neural network takes a few milliseconds to perform signal detection and classification as compared to traditional methodologies based on the iterative and algorithmic signal search and signal detection and classification.

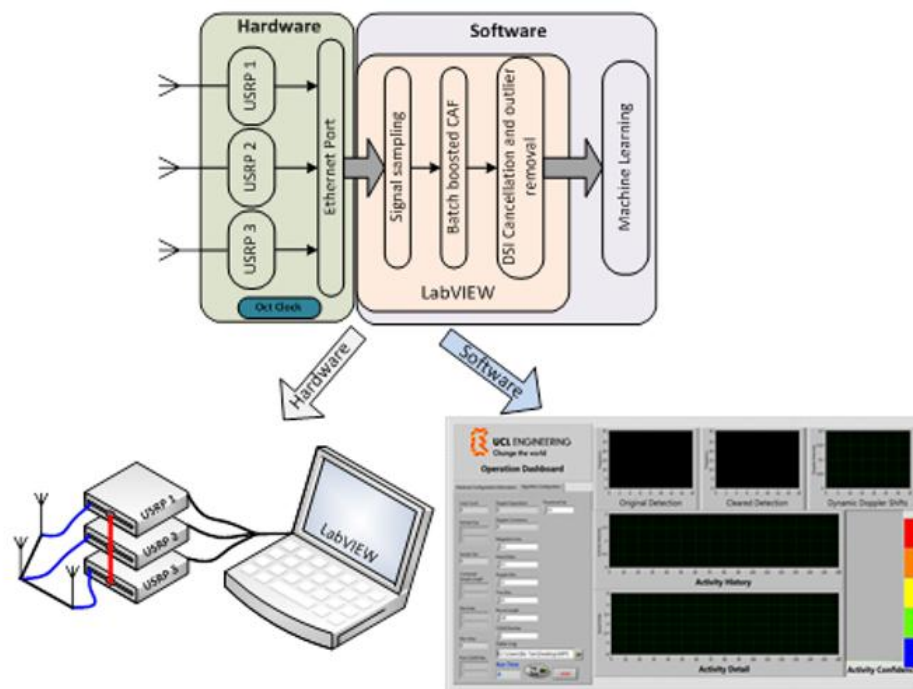


Figure 1: Deep learning allows training of RF signals in just a few seconds after the signal capture. Source: National Instruments

It is important to note that such gains also significantly reduce power consumption and computational requirements. Moreover, a learned communication system allows wireless designers to prioritize key design parameters such as throughput, latency, range and power consumption.

More importantly, deep learning-based training models facilitate a better awareness of the operational environment and promise to offer end-to-end learning for creating an optimal radio system. Case in point: a training model that can jointly learn an encoder and decoder for a radio transmitter and receiver while encompassing RF components, antennas and data converters.

Additionally, what technologies like deep learning promise in the wireless realm is the commoditization of the physical layer (PHY) and signal processing design. Combining deep learning-based sensing with active radio waveforms creates a new class of use cases that can intelligently operate in a variety of radio environments.

The following section will present a couple of design case studies that demonstrate the potential of AI technologies in wireless communications.

Two design case studies

First, the OmniSIG software development kit (SDK) from DeepSig Inc. is based on deep learning technology and employs real-time signal processing to allow users to train signal detection and classification sensors.

DeepSig claims that its OmniSIG sensor can detect Wi-Fi, Bluetooth, cellular and other radio signals up to 1,000 times faster than existing wireless technologies. Furthermore, it enables users to understand the spectrum environment and thus facilitate contextual analysis and decision making.

ENSCO, a U.S. government and defense supplier, is training the OmniSIG sensor to detect and classify wireless and radar signals. Here, ENSCO is aiming to deploy *AI-based capabilities* to overcome the performance limitations of conventionally designed RF systems for signal intelligence.

What DeepSig's OmniPHY software does is allow users to learn the communication system, and subsequently optimize channel conditions, hostile spectrum environments and hardware performance limitations. The applications include anti-jam capabilities, non-line-of-sight communications, multi-user systems in contested spectrums and mitigation of the effects of hardware distortion.

Another design case study showing how AI technologies like deep learning can impact future hardware architectures and designs is the passive Wi-Fi sensing system for monitoring health, activity and well-being in nursing homes (Figure 2). The continuous surveillance system developed at Coventry University employs gesture recognition libraries and machine learning systems for signal classification and creates a detailed analysis of the Wi-Fi signals that reflect off a patient, revealing patterns of body movements and vital signs.

Residential healthcare systems usually employ wearable devices, camera-based vision systems and ambient sensors, but they entail drawbacks such as physical discomfort, privacy concerns and limited detection accuracy. On the other hand, a passive Wi-Fi sensing system, based on activity recognition and through-wall respiration sensing, is contactless, accurate and minimally invasive.

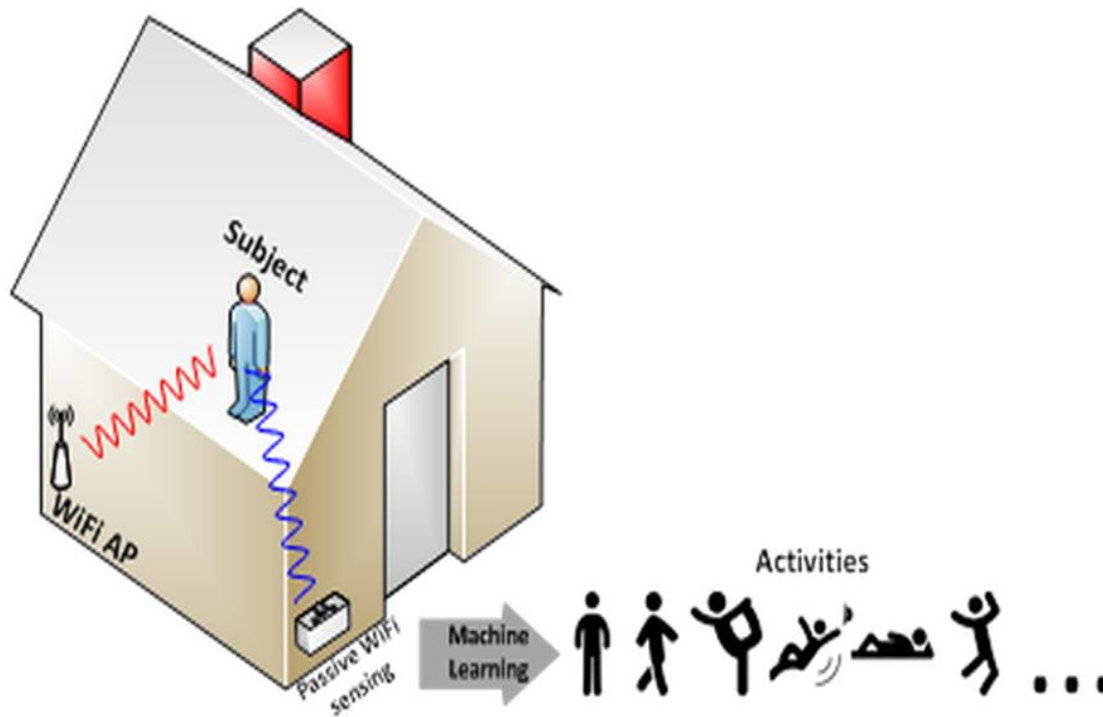


Figure 2: Machine learning allows designers to classify radio signals for recognizing daily activities from the Doppler-time spectral map. Source: National Instruments

The passive Wi-Fi sensing for nursing homes has its roots in a research project on passive Wi-Fi radar carried out at University College London. The passive Wi-Fi radar prototype —based on software-defined radio (SDR) solutions from National Instruments (NI) — is completely undetectable and can be used in military and counterterrorism applications.

USRP transceiver plus LabVIEW

A passive Wi-Fi sensing system is a receive-only system that measures the dynamic Wi-Fi signal changes caused by moving indoor objectives across multiple path propagation. Here, AI technologies like machine learning allow engineers to use frequency to measure the phase changing rate during the measurement duration as well as Doppler shift to identify movements.

Machine learning algorithms can establish the link between physical activities and the Doppler-time spectral map associated with gestures such as picking things up or sitting down. The phase of the data batches is accurate enough to discern the small body movements caused by respiration.

Coventry University built a prototype of a passive Wi-Fi sensing system using Universal Software Radio Peripheral (USRP) and LabVIEW software to capture, process and interpret the raw RF signal samples. LabVIEW, an intuitive graphical programming tool for both processors and FPGAs, enables engineers to manage complex system configurations and adjust signal processing parameters to meet the exact requirements.

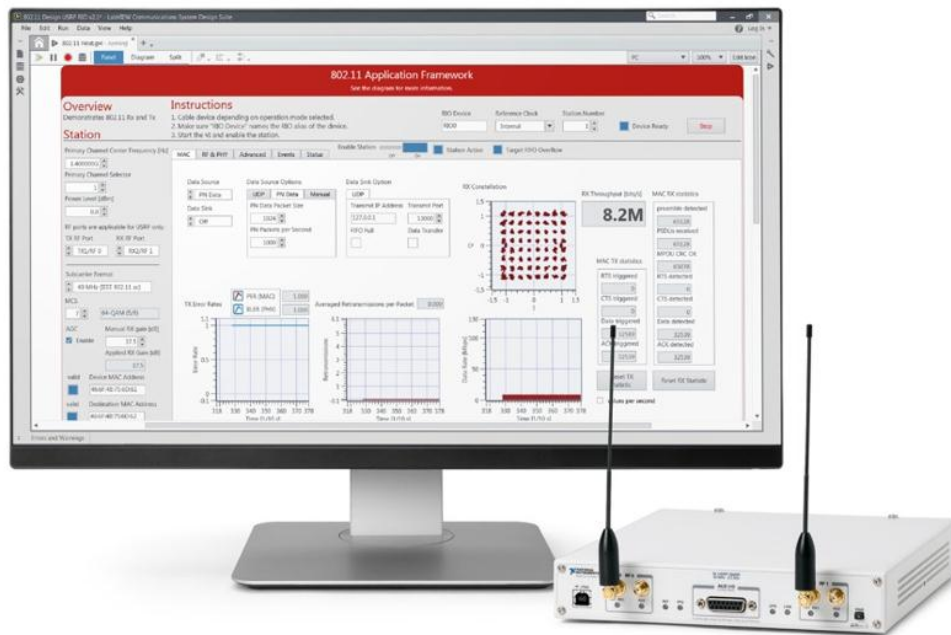


Figure 3: The USRP transceiver interfaced with LabVIEW software allows engineers, scientists and students to develop algorithms for next-generation wireless technologies. Source: National Instruments

On the other hand, USRP is an SDR-based tunable transceiver that works in tandem with LabVIEW for prototyping wireless communication systems. It has already been used in prototyping wireless applications such as FM radio, direction finding, RF record and playback, passive radar and GPS simulation.

Engineers at Coventry University have used USRP to capture the raw RF samples and deliver them to the LabVIEW application for speedy signal processing. They have also dynamically changed the data arrays and batch size of analysis routines to adapt the system to slow and fast movements.

Engineers were able to interpret some captured signals and directly link the periodic change of batch phase with gestures and respiration rate. Next, they examined if the phase of the data batches was accurate enough to discern the small body movements caused by respiration.

AI: The next wireless frontier

The above design examples show the potential of AI technologies like machine learning and deep learning to revolutionize the RF design, addressing a broad array of RF design areas and creating new wireless use cases.

These are still the early days of implementing AI in wireless networks. But the availability of commercial products such as USRP suggests that the AI revolution has reached the wireless doorstep.

Reference :

- [1] arXiv:2003.00866v1 [cs.NI] 24 Feb 2020
- [2] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to pareto-optimal wireless networks," IEEE Communications Surveys & Tutorials, 2020.
- [3] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," arXivpreprint arXiv:1902.10265, 2019.
- [4] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G—AI emp

The age of Virtual Reality, Augmented Reality and Mixed Reality

Sohan Goswami
Lecturer, DCST

A) Virtual Reality: This is the century of modern science and technology and Virtual Reality. Virtual Reality, or VR, is a simulated and immersive experience projected by a device into the user's sight. All you need is a headset projecting you into a simulation via a viewfinder. That's exactly what VR promises, and much more.

VR is the most widely known of these technologies. It is fully immersive, which tricks your senses into thinking you're in a different environment or world apart from the real world. Using a head-mounted display (HMD) or headset, you'll experience a computer-generated world of imagery and sounds in which you can manipulate objects and move around using haptic controllers while tethered to a console or PC.

There are three main types of virtual reality used today to transform the world around us, including non-immersive, semi-immersive, and fully-immersive simulations.

- 1) **Fully-Immersive VR:** Fully-immersive simulations give users the most realistic experience possible, complete with sight and sound. The VR headsets provide high-resolution content with a wide field of view. Whether you're flying or fighting the bad guys, you'll feel like you're really there.



- 2) **Semi-Immersive VR:** Semi-immersive experiences provide users with a partially virtual environment to interact with. This type of [VR is mainly used for educational](#) and training purposes and the experience is made possible with graphical computing and large projector systems.

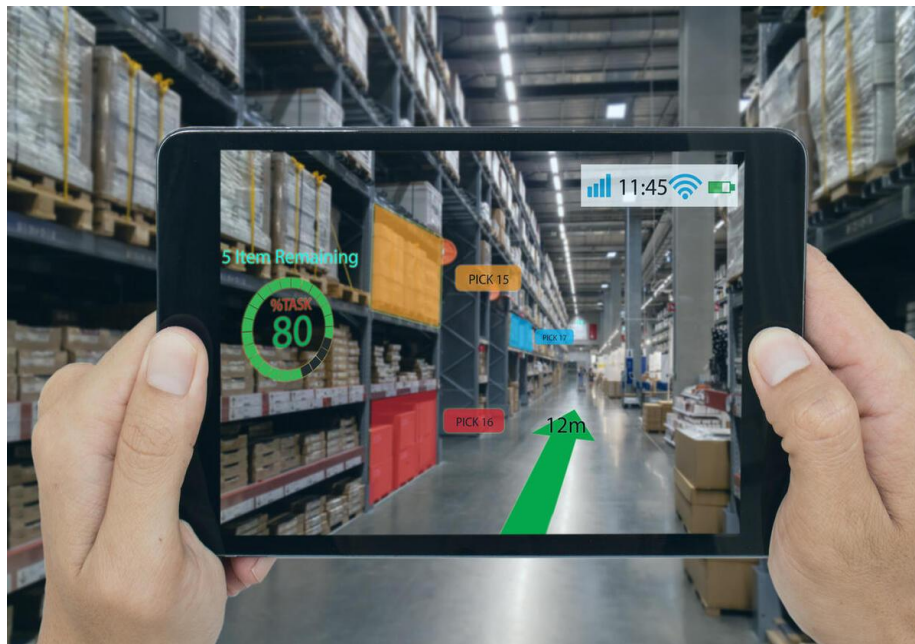


In this example, the instruments in front of the pilot are real and the windows are screens displaying virtual content.

- 3) **Non-Immersive VR:** The average video game is technically considered a non-immersive virtual reality experience. Think about it, you're sitting in a physical space, interacting with a virtual one.



B) Augmented Reality: Augmented Reality overlays digital information on real-world elements. Pokémon GO* is among the best-known examples. Augmented reality keeps the real world central but enhances it with other digital details, layering new strata of perception, and supplementing your reality or environment.



Augmented reality (AR) is one of the biggest technology trends right now, and it's only going to get bigger as AR ready smartphones and other devices become more accessible around the world. AR let us see the real-life environment right in front of us—trees swaying in the park, dogs chasing balls, kids playing soccer—with a digital augmentation overlaid on it.

Perhaps the most famous example of AR technology is the mobile app Pokémon Go, which was released in 2016 and quickly became an inescapable sensation. In the game, players locate and capture Pokémon characters that pop up in the real world—on your sidewalk, in a fountain, even in your own bathroom.

C) Mixed Reality: MR brings together real world and digital elements. In mixed reality, you interact with and manipulate both physical and virtual items and environments, using next-generation sensing and imaging technologies. Mixed Reality allows you to see and immerse yourself in the world around you even as you interact with a virtual environment using your own hands—all without ever removing your headset. It provides the ability to have one foot (or hand) in the real world, and the other in an imaginary place, breaking down basic concepts between real and imaginary, offering an experience that can change the way you game and work today.

Mixed Reality is the merge of real and virtual worlds to produce new environments and visualizations where physical and digital objects co-exist and interact in real time. For example – picture a surgeon having a digital overlay while performing an operation, providing detailed live information on the process and the current state of the patient like blood pressure and other vital insights.



Microsoft Hololens: The **Hololens** is **Microsoft's** mixed reality application. Using multiple sensors, advanced optics, and holographic processing that melds seamlessly with its environment, These holograms can be used to display information, blend with the real world, or even simulate a virtual world.



HoloLens allows users to experience [3D](#) holographic images as though they are a part of their environment. This level of immersion enables new forms of computing in which the user's desktop could be the living room. You might stream Netflix on a wall or build a Minecraft castle on your coffee table, as high resolution holograms.

Mixed reality is a technology of the future that can be used in a number of applications in various industries such as education, entertainment, and healthcare. The following are a few examples of future mixed reality applications:

Immersive movies:

A movie trailer launch is an important promotional event. Everything related to the trailer launch event needs to be perfect to generate a pre-release buzz for the movie. We all are aware of how movie actors hardly arrive on time at any particular event. Mixed reality technology can be used by the production houses for trailer launches with the movie actors making an appearance at the event remotely. Likewise, the press conference after the trailer launch can also be conducted virtually.

Educational classes

One of the most important factors that usually helps students understand a particular topic or concept related to a subject is the practical demonstration of the concept. For instance, if the topic is based on

the seven wonders of the world a teacher with mixed reality and AR technology can guide them through the seven wonders of the world. Alternatively, they can let the students explore the places in a three-dimensional, 360-degree environment with VR-enabled headsets. With the use of mixed reality technology, students do not just visually experience the place, they actually feel they are in the place. An app developed by Google helps create an interactive, virtual environment in the classroom and allows students to explore any historical landmark, get a clear view of underwater life, and even visit outer space.

Corporate meetings

Have you ever thought about the possibility of a meeting taking place with all the members attending it remotely? There is a high possibility such events will actually happen in the future. Microsoft is currently working on a project called 'Holoportation,' which utilizes mixed reality technology. The execution of this application could allow individuals with headset device such as HoloLens to remotely participate in the meeting and interact with each other with the help of 3D motion capture system.

Surgical applications

The use of mixed reality technology in medical applications can help transform the healthcare sector completely. By making use of VR headsets, with the incorporation of AR technology, surgeons could easily operate on their patients in a much more effective way than usual Political Campaigns.

Interactive gaming

One of the sectors that is constantly evolving with technology is the gaming industry. Though Pokémon Go, which completely incorporated augmented reality technology, has been one of the most popular games in recent times, the gaming world is now trying to experiment with cutting edge technology like mixed reality.

Event engagement

One of the most popular events around the world that attracts a lot of eyeballs is a music festival. The event coordinators ensure that every arrangement is made properly and all the minor details are in place to make the event successful. Mixed reality technology can not only be used for visual experiences, but the technology has the potential to affect our taste buds. An example is the 'Taste Buddy' gadget, which can help electrify our taste buds in the future. The gadget generates electrical and thermal signals that could help stimulate our taste buds. The use of Taste Buddy gadget that incorporates mixed reality could help trick our taste buds and make us feel like we're tasting our favourite foods such as chocolate, even though we are actually eating a vegetable. Here, mixed reality technology can help people switch to a healthier lifestyle.



Hello! Android users. You might have heard about rooting android phones. It sounds cool but you might be afraid of doing that. Well it's a really easy process and if you do it carefully the no harm will be done to your phone. For those who don't know about rooting, well rooting is basically a process that allows you to attain root access to the android operating system. It sounds stuffy but it's just the process that you should do if you want to do some sort of custom OS installation, use modified apks, start hacking through your phone etc.

Since you have reached reading this far, I am sure you are interested. Nowadays majority people are using Xiaomi phones, so my tutorial would be based on a Xiaomi device. There are three steps to root your Xiaomi device.

1. Preparing Environment

To root your Xiaomi Device, you must have a computer and a data transferable cable.

- First turn the developer options on (tap on MIUI version 7 times).
- Then find the developer options on settings. Turn on OEM unlocking, USB Debugging and tap the unlock bootloader button (open MI unlock status to find that button)

****Make sure that your MI account is added to your phone.**

- Now come to your computer.
- Download
 - 15 sec ADB installation executable file
 - Platform tools suitable for your phone
 - OrangeFox Recovery.zip (orangefox.download)
 - MI Unlocker Tool.zip (en.miui.com/unlock)
 - Magisk Installer.zip <https://github.com/topjohnwu/Magisk/releases/download/v20.4/Magisk-v20.4.zip>

2. Unlocking Bootloader

Don't get afraid, unlocking bootloader will no longer void your warranty since 2020. Before doing this make sure you backed up all your important data from your phone because it will wipe your phone.

- Press and hold power and volume+ button to enter fastboot mode and put your phone aside.
- On your PC and extract MI Unlocker Tool.zip
- Open the application or executable file from the extracted folder.
- Now login in this app with your MI account ID and Password.
- Once you are done setting up these, connect your phone with your PC.
- Then the unlock button will be visible in the MI unlocker tool on PC
- Tap Unlock and press ok.

Your phone should be unlocked now. To verify you'll see unlocked logo while booting.

3. Installing Magisk

To root Xiaomi devices, you have to install magisk.

- Put your phone on fastboot mode and come to your PC
- Install 15 sec ADB installation executable file
- Extract Platform tools and OrangeFox recover zip files.
- Copy recovery.img from OrangeFox folder to Platform tools folder.
- Open CMD from Platform tools folder (shift+ right click
→Open Command Prompt here.
- Type fastboot devices to check your device is connected or not.
- Type fastboot boot <location of the recovery.img from platform tools>
- When you are finally booted into OrangeFox recovery Mode copy the Magisk Installer.zip to your phone.
- Find that file on your phone while your phone is OrangeFox recovery.
- Install that file. (Uncheck all the boxes which will popup while installation).

Finally, Your Phone is rooted properly. You can verify by installing app called Root Checker.

INTRODUCTION

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

FEATURES

Features Of Cryptography are as follows:

1. Confidentiality:

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. Integrity:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. Non-repudiation:

The creator/sender of information cannot deny his or her intention to send information at later stage.

4. Authentication:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

1. Symmetric Key Cryptography:

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

WORKING APPLICATION

The most important principle to keep in mind is that you should never attempt to design your own cryptosystem. The world's most brilliant cryptographers (including Phil Zimmerman and Ron Rivest) routinely create cryptosystems with serious security flaws in them. In order for a cryptosystem to be deemed "secure," it must face intense scrutiny from the security community. Never rely on security through obscurity, or the fact that attackers may not have knowledge of your system. Remember that malicious insiders and determined attackers will attempt to attack your system.

The only things that should be "secret" when it comes to a secure cryptosystem are the keys themselves. Be sure to take appropriate steps to protect any keys that your systems use. Never store encryption keys in clear text along with the data that they protect. This is akin to locking your front door and placing the key under the doormat. It is the first place an attacker will look. Here are three common methods for protecting keys (from least secure to most secure):

1. Store keys in a filesystem and protect them with strong access control lists (ACLs). Remember to adhere to the principal of least privilege.
2. Encrypt your data encryption keys (DEKs) with a second key encrypting key (KEK). The KEK should be generated using password-based encryption (PBE). A password known to a minimal number of administrators can be used to generate a key using an algorithm such as bcrypt, scrypt, or PBKDF2 and used to bootstrap the cryptosystem. This removes the need to ever store the key unencrypted anywhere.
3. A hardware security module (HSM) is a tamper-resistant hardware appliance that can be used to store keys securely. Code can make API calls to an HSM to provide keys when needed or to perform decryption of data on the HSM itself.

Make sure that you only use algorithms, key strengths, and modes of operation that conform to industry best practices. Advanced encryption standard (AES) (with 128, 192, or 256-bit keys) is the standard for symmetric encryption. RSA and elliptical curve cryptography (ECC) with at least 2048-bit keys are the standard for asymmetric encryption. Be sure to avoid insecure modes of operation such as AES in Electronic Codebook (ECB) mode or RSA with no padding.

ADVANTAGES OF CRYPTOGRAPHY

Cryptography is an essential information security tool. It provides the four most basic services of information security –

- Confidentiality – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- Authentication – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- Data Integrity – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

- Non-repudiation – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.
- All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

DISADVANTAGES OF CRYPTOGRAPHY

Modern cryptography provides a robust set of techniques to ensure that the malevolent intentions of the adversary are thwarted while ensuring the legitimate users get access to information. These are the issues that affect the effective use of information

- A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision- making. The network or the computer system can be attacked and rendered non-functional by an intruder.
- High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.
- Another fundamental need of information security of selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.
- Cryptography comes at cost. The cost is in terms of time and money –Addition of cryptographic techniques in the information processing leads to delay.The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

CONCLUSION

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism.

Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable.

Ethical hacking is a structured hacking performed to expose vulnerabilities in a system, using tools and techniques with the organization's knowledge and approval.

Hacking is usually doing something which you are not allowed to do. For example viewing a page that you don't have permission or, viewing some information or, gaining access to a computer that you don't have permission too.

Hacking is the act of finding a clever solution to programming issue. So, a hacker is known as clever programmer.

Types of Ethical Hacking

- Email Hacking
- System Hacking
- Web Server Hacking
- Web Application Hacking
- Social Engineering

Types of Hackers

- White Hat
- Black Hat
- Grey Hat

White Hat Hacker - White Hat Hackers do not intend to harm the system or organization but they do so, officially, to penetrate and locate the vulnerabilities, providing solutions to fix them and ensure safety.

Black Hat Hacker - Black Hat Hackers or non-ethical hackers perform hacking to fulfill their selfish intentions to collect monetary benefits.

Grey Hat Hacker - Grey Hat Hackers are the combination of white and black hat hackers. They hack without any malicious intention for fun. They perform the hacking without any approval from the targeted organization.

Five Phases of Ethical Hacking

- Planning and Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Analysis

Hacking Techniques

Keylogger: Keylogger is a computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

DDoS Attack: Denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Waterhole Attack: Watering hole attack works by identifying a website that's frequented by users within a targeted organisation, or even an entire sector, such as defence, government or healthcare. That website is then compromised to enable the distribution of malware.

Eavesdropping: An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device.

Bait and Switch: Bait & Switch is a type of fraud that uses relatively trusted avenues - ads - to trick users into visiting malicious sites.

Virus: Virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.

It infects other programs, alters data, transforms itself, encrypts itself, corrupt files and programs, self propagates.

Advantages of Ethical Hacking

Most of the benefits of ethical hacking are obvious, but many are overlooked. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include:

- Fighting against terrorism and national security breaches.
- Having a computer system that prevents malicious hackers from gaining access.
- Having adequate preventative measures in place to prevent security breaches.

Disadvantages of Ethical Hacking

As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. The possible drawbacks of ethical hacking include:

- The ethical hacker using the knowledge they gain to do malicious hacking activities.
- Allowing the company's financial and banking details to be seen.
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system.
- Massive security breach.

10 Commandments of Ethical Hacking

- Set your own goals
- Plan your work
- Always obtain permission
- Work ethically
- Maintain a record of ethical hacking
- Respect others privacy
- Resist the urge
- Adopt a scientific process
- Restrict when collecting the tools
- Report all your findings

Best Ethical Hacking Tools

- Kiuwan
- Nmap
- Metasploit
- Intruder
- Aircrack-Ng
- Wireshark
- Ettercap

Digital Image Processing (DIP) is a software which is used to manipulate the digital images by the use of computer system. It is also used to enhance the images, to get some important information from it.

It is also used in the conversion of signals from an image sensor into the digital images.

A certain number of algorithms are used in image processing.

Digital Image Processing provides a platform to perform various operations like image enhancing, processing of analog and digital signals, image signals, voice signals etc.

It provides images in different formats.

After the invention of digital computers, digital image processing took various advantages over analog image processing. A broad range of techniques and methods, in the form of a variety of algorithms, came into existence. Since images are defined over two dimensions (and perhaps more) digital image processing may be modeled in the form of multidimensional systems. Digital image processing has evolved rapidly with the development of computers.

History of Digital Image Processing

Early 1920s

Bartlane cable picture transmission system

- used to transmit newspaper images across the Atlantic.

- images were coded, sent by telegraph, printed by a special telegraph printer. - took about three hours to send an image, first systems supported 5 gray levels

1964 – NASA's Jet Propulsion Laboratory began working on computer algorithms to improve images of the moon.

- images were transmitted by Ranger 7 probe.

- corrections were desired for distortions inherent in on-board camera.

[Aaron Klug Invents Digital Image Processing for Two-Dimensional Images.]

Working of DIP

Digital image processing is the use of computer algorithms to create, process, communicate, and display digital images. ... Convert signals from an image sensor into digital images. Improve clarity, and remove noise and other artifacts. Extract the size, scale, or number of objects in a scene.

Some techniques which are used in digital image processing :

- Neural networks
- Anisotropic diffusion
- Pixelation
- Hidden Markov models
- Image editing
- Image restoration

- Independent component analysis
- Linear filtering
- Partial differential equations
- Self-organizing maps
- Wavelets

Advantages of DIP

1. It improves the visual quality of an image and the distribution of intensity.
2. Mathematical and logical operations can be performed on an image like addition subtraction, OR etc.
3. It can process an image in such a way that the result is more suitable than the original image
4. An image can be easily modified using a number of techniques
5. The image compression technique reduces the amount of data required to represent a digital image.

Disadvantages of DIP

1. The initial cost can be high depending on the system used.
2. If computer is crashes then pics that have not been printed and filed into Book Albums that are lost.
3. Digital cameras which are used for digital image processing have some disadvantages like:
4. Memory Card Problems
5. Higher Cost
6. Battery Consumption

Applications of Digital Image Processing

- Image sharpening and restoration
- Medical field
- Remote sensing
- Transmission and encoding
- Machine/Robot vision
- Color processing
- Pattern recognition
- Video processing
- Microscopic Imaging
- Others

Digital image processing allows the use of much more complex algorithms. Hence it offers both -more sophisticated performance at simple tasks -the implementation of methods which would be impossible by analog means.

Robotic process automation (or RPA) is a form of business process automation technology based on metaphorical software robots (bots) or on artificial intelligence (AI)/digital workers. It is sometimes referred to as software robotics (not to be confused with robot software).

RPA is the technology that allows the automation of the task in exactly the way how a human does. A robot in robotic process automation does not mean that literally robots are going to replace human beings, but it means a computer program that imitates human actions.

In other words, we can say that RPA is a software program that imitates human actions while interacting with a computer application and accomplishing the automation of repetitive and rule-based processes. RPA can be used to automate the labour intensive tasks such as back office processes, data entry, data validation etc.

History of RPA (Robotic Process Automation)

RPA is the combination of several technologies, brought together under one toolkit for different automation purposes. Though the term 'RPA' emerged in the early 2000s, the initial development was started after the 1990s.

'Machine Learning (ML)' is one of those technologies that helped towards innovation, which eventually lead to the creation of RPA. In 1959, 'Arthur Samuel' developed Machine Learning. Machine Learning allowed computers to perform several critical tasks, such as translation and text summarization, etc. However, there were limits on how computers could process language. It led to the development of 'Natural Language Processing (NLP),' which helped computers to understand and process human language more accurately. In 1960, NLP combined 'AI (Artificial Intelligence)' for establishing the interactions between computers and human languages. Then, the technology progressed further towards the establishment of RPA, and there were few more developments in the 1990s.

Blue prism released their first product in 2003, UiPath(**It is a global software company that develops a platform for robotic process automation**)and Automation anywhere released their automation libraries around the same time (all companies were founded a bit earlier).

Working of RPA

With the name of RPA, many people may think about physical robots performing day to day tasks. However, RPA does not use physical robots to automate tasks. It does not replace humans with actual robots. The term 'robot' in Robotic Process Automation is a software running on physical or virtual machines. Such software help in configuring automation workflows to automate business operations.

RPA is the use of computer software 'robots' to handle repetitive, rule-based digital tasks such as filling in the same information in multiple places, reentering data, or copying and pasting. It enables organizations to give more and more of the mundane admin work over to machines that can handle it well and in full compliance.

This enables an organization to achieve cost efficiencies by streamlining processes and enhancing accuracy. As importantly, it enables humans to focus on work that requires judgment, creativity and interpersonal skills rather than on routine processes.

RPA features

RPA offers some amazing features that'll change the concept of working in the industry. Automation technology is not new but RPA offers zero percent errors and that is why bigger industries rely on RPA. The process also offers scalability with deployment. It offers great performance and efficiency in a working environment. The reporting and analysis tasks performed by RPA eliminate the need for extra monitoring.

Key characteristics of RPA :

- Security and source controlled
- Computer-coded software
- Programs imitating human interaction with applications
- Cross-functional application
- Virtual workforce controlled by business operations
- Agile and non-invasive, works with existing IT architecture and governance

Advantages of RPA

Cost Effective

- 25-50% Reduction in Operational • 24/7 Availability

Accuracy & Quality

- Nearly 100% Accuracy, Ensuring Compliance • Eliminates Human-Error

Employee Productivity

- Frees Workforce from Mundane Tasks • Create Space for Innovation and Creativity Increased

Customer Satisfaction

- Enable round-the-clock Customer Services • Improved customer / client interaction

Faster

- 1 Bot can Process Large Amount of Work • Quick Turn-Around Time

Reconciliation from Multiple Systems

- Tally Data and Information from Multiple Systems • Enable Integration of Processes

Better IT Support and Management

- Improved Operational Quality of Service Desk • Handles Short-Term Spikes

Disadvantages of RPA

- Potential Job Losses
- Initial Investment costs
- Hiring Skilled Staff
- Employee Resistance
- Process Selection

Applications of RPA

Industrial usage

❖ Healthcare

- Patient Registration • Billing

❖ Insurance

- Claims Processing & Clearance • Premium Information

❖ Telecom

- Service Order Management • Quality Reporting

- ❖ Banking and Financial Services
 - Cards activation • Frauds claims • Discovery
- ❖ Government
 - Change of Address • License Renewal

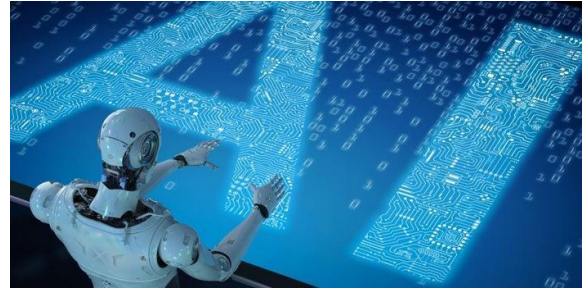
General Use of RPA

1. Emulates Human Action
2. Product management
3. Perform Multiple Tasks
4. 'Virtual' system integration
5. Revenue forecasting
6. Data migration
7. Technical debt management

Thus, due to the various benefits of RPA, its utilization is gradually increasing in the market worldwide. Most of the organizations are already implementing the RPA technology, as it optimizes the cost and frees the other resources.

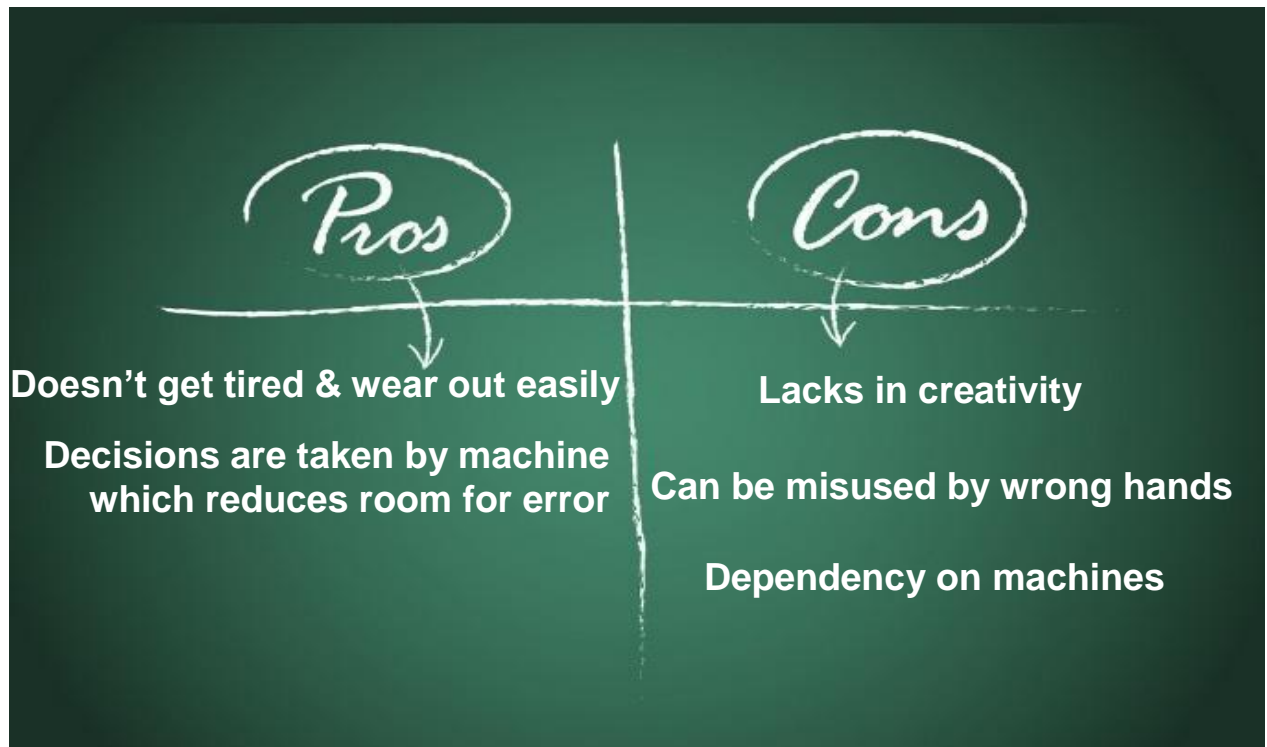
What is **Artificial Intelligence**: -

Artificial Intelligence (AI) is truly a revolutionary feat of computer science set to become a core component of all modern software over the coming years and decades. In general terms AI refers to computational tools that are able to substitute for human intelligence in the performance of certain tasks. It is sometimes also called machine learning.

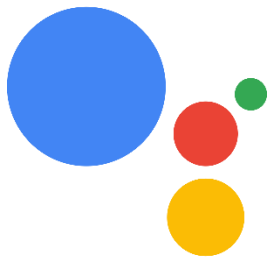


<i>MYTH</i>	<i>FACT</i>
AI is replacing all jobs	Only low skilled and manual workers will be replaced by AI and Automation
Super intelligent computers will become better than humans at doing anything we can do	Essentially super humans who can beat us at pretty much anything
AI algorithms can magically make sense of any and all of your messy data	AI is not “load and go” and the quality of the data is more important than the algorithm
You need data scientists, machine learning experts and huge budgets to use AI for the businesses	Many tools are increasingly available to business users and don’t require Google-sized investments
“Cognitive AI” technologies are able to understand and solve new problems the human brain can	“Cognitive” technologies can’t solve problems they weren’t designed to solve
AI will displace humans and make contact center jobs obsolete	AI is no different from other technological advances in that it helps humans become more effective and processes more efficient

Pros and Cons of AI: -



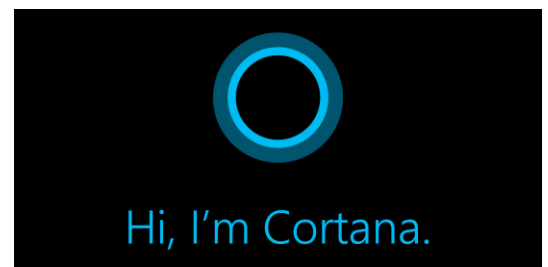
Example of Some popular **Artificial Intelligence (AI)** based assistant services: -



Google Assistant



Siri



Cortana



Alexa



Bixby

Google Assistant: - Google Assistant is an artificial intelligence powered virtual assistant developed by Google that is primarily available on mobile and smart home devices. Assistant initially debuted in May 2016 as part of Google's messaging app Allo and its voice-activated speaker Google Home. It began to be deployed on Android devices in February 2017, including third party smartphones and Android Wear (now Wear OS) and was released as a standalone app on the iOS operating system in May 2017. Later it became available in KaiOS, Linux etc. Users primarily interact with the Google Assistant through natural language, though keyboard input is also supported. Google Assistant is able to search the internet, schedule events, and alarms, adjust hardware settings on user's device and show information from user's Google account. It is also able to identify objects and gather visual information through the device's camera and support purchasing products and sending money, as well as identifying songs.

Official Website: <https://assistant.google.com/>

Siri: - Siri is a virtual assistant that is part of Apple Inc.'s iOS, iPadOS, watchOS, macOS and tvOS operating system. The assistant uses voice queries and a natural language user interface to answer questions, make recommendations and perform actions by delegating requests to a set of Internet services. The software adapts to users' individual language usages, searches and preferences with continuing use. Returned results are individualized. Siri was first released on 12th October 2011. It is supported from iOS 5 onward and macOS Sierra onward, tvOS (all versions), watchOS (all versions). The voice assistant was released as an app for iOS in February 2010 and it was acquired by Apple two months later. Siri was then integrated into iPhone 4S at its release in October 2011. At that time, the separate app was also removed from Appstore. Siri has since become an integral part of Apple's products, having been adapted into other hardware devices over the years, including newer iPhone models, as well as iPad, iPod Touch, iMac, MacBook, AirPods, Apple TV and HomePod. Siri supports a wide range of user commands, including performing phone actions, checking basic information, scheduling events and reminders, handling device's settings, searching the Internet, navigating areas, finding information on entertainment, and is able to engage with iOS-integrated apps. With the release of iOS 10 in 2016, Apple opened up limited third-party access to Siri, including third-party messaging apps, as well as payments, ride-sharing, and Internet calling apps. With the release of iOS 11, Apple updated Siri's voices for more clear, human voices, started supporting follow-up questions and language translation, and additional third-party actions.

Official Website: <https://www.apple.com/siri/>

Cortana: - Cortana is a virtual assistant created by Microsoft for Windows 10, Windows mobile, Microsoft Band, Surface Headphones, Xbox One, iOS, Android, Windows Mixed Reality, Amazon Alexa. Though Microsoft removed Cortana from Android and iOS from 31st January 2020, it was first released on 2nd April 2014. Cortana was first demonstrated for the first time at the Microsoft BUILD Developer conference in San Francisco. It has been launched as a key ingredient of Microsoft's planned "makeover" of the future operating systems for Windows Phone and Windows. Cortana can set reminders, recognize natural voices without the requirement for keyboard input and answer questions using information and web results from the Bing search engine. The development of Cortana started in 2009 in the Microsoft speech products team with general manager Zig Serafin and Chief Scientist Larry Heck. It is named after Cortana, a synthetic intelligence character in Microsoft's Halo video game franchise originating in Bungie folklore with Jen Taylor, the character's voice actress, returning to voice the personal assistant's US-specific version.

Official Website: <https://www.microsoft.com/en-us/windows/cortana>

Alexa: - Amazon Alexa is simply known as Alexa, is a virtual assistant AI technology developed by Amazon, first used in the Amazon Echo smart speakers developed by Amazon Lab126. It is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audiobooks and providing weather, traffic, sports and other real time information such as news. Alexa can also control several smart devices using itself as a home automation system. Users are able to extend the Alexa capabilities by installing “Skills” (additional functionality developed by third-party vendors, in other settings more commonly called apps such as weather programs and audio features). Most devices with Alexa allow users to activate using a wake-word (such as Alexa); other devices require the user to push a button to activate Alexa’s listening mode. It was initially released on 6th November 2014. It is capable on various operating system like FireOS 5.0 or later, iOS 11.0 or later, Android 4.4 or Later.

Official Website: <https://developer.amazon.com/alexa>

Bixby: - Bixby is a virtual assistant developed by Samsung Electronics. On 20th March 2017, Samsung announced the voice powered digital assistant named “Bixby”. Bixby was introduced alongside the Samsung Galaxy S8 and S8+, as well as Samsung Galaxy Tab A during the Samsung Galaxy Unpacked 2017 event, which was held on 29th March 2017. Bixby can also be sideload on older Galaxy devices running Android Nougat. Bixby represents a major reboot for S Voice, Samsung’s voice assistant app introduced in 2012 with the Galaxy s III. In May 2017, Samsung announced that Bixby would be coming to its line of Family Hub 2.0 refrigerators, making it the first non-mobile product to include the virtual assistant. In October 2017, Samsung announced the release of Bixby 2.0 during its annual developer conference in San Francisco. The then-new version was rolled out across the company’s line of connected products, including smartphones, TVs and refrigerators. Also, third parties are allowed to develop applications for Bixby using the Samsung Developer Kit. Bixby is capable on Android and Tizen (Samsung’s own operating system) OS.

Official Website: <http://bixby.samsung.com/>

References:

- https://en.wikipedia.org/wiki/Google_Assistant
- <https://en.wikipedia.org/wiki/Siri>
- <https://en.wikipedia.org/wiki/Cortana>
- https://en.wikipedia.org/wiki/Amazon_Alexa
- [https://en.wikipedia.org/wiki/Bixby_\(virtual_assistant\)](https://en.wikipedia.org/wiki/Bixby_(virtual_assistant))

3-D Home Printers Could Change Economy

Milan Halder
DCST, 2nd year

When your favorite gadget of the future breaks, you might select a replacement model online, download its design file and make a true 3-D replacement on your home printer

Thanks to falling prices and wider application of an industrial technology called 3-D printing (among other things), this option might be a reality for consumers in a few years.

Instead of stamping or casting to create objects using tools, dies and forms that were laboriously created for the task, each object is basically printed—built thin layer by thin layer directly from a computer-aided design, or CAD, file using various high-accuracy deposition methods.

Sintering, for instance, deposits layers of fine particles that are heated until they bind to adjacent particles. Stereo-lithography, meanwhile, uses a laser to harden a layer of an object on the surface of a pool of special resin. The object is then lowered slightly, and the next layer is created. Altogether, 3-D printing technologies can create things out of plastics, metal and ceramics, and some methods can add photo-realistic coloring.

More importantly, prices for 3-D printing machines have been falling rapidly, reaching \$20,000, and the day is foreseeable when they will fall below \$1,000 and become home appliances, says Phil Anderson of the School of Theoretical and Applied Science at Ramapo College in New Jersey.

The results, he warned, could be economically "disruptive."

"If you can make what you need in your own home quickly, then manufacturers become designers, with no need for factories, warehouses or shipping," Anderson told

Drawbacks to 3-D printing include time (aside from creating the data file, each object takes several hours to print and then usually requires additional curing), power consumption (metal objects especially require a lot of heat), size (current low-end machines have a work-space measuring 10 inches per side, so that anything larger would have to be made in segments) and the price of the specialized raw material.

Accuracy, surface finish and strength are not yet as good at the low-end as at the high-end, says industrial consultant Terry Wohlers.

3-D printers cheap enough for the home market could appear in four or five years, Wohlers said, though Anderson puts that figure at 15 years. However, that does not mean they will be in every home, churning out kitchenware or car parts on demand.

Other than dedicated tinkerers, video gamers will be the initial consumer market, Wohlers said.

"There are millions of people playing video games that often involve the creation of elaborate action figures," he noted. "I think the first wave will be the addition of a button to those games that says 'build me.' The figure would arrive in the mail, and you could get a six-inch figure for \$25 to \$100."

Today, making a figurine through a 3-D printing service bureau could cost something on the order of \$500, but Wohlers expects volume would drive costs down considerably.

CYBER SECURITY

“A BOON TO THE DIGITALLY EMERGING ERA”

Debajyoti Banerjee,
DCST, 3rd year

Now, before directly jumping into the discussion on the topic let us see an example of cyber-attack and how it started and why is it became a necessity for everybody to rely on cyber security who is using modern technology and gadgets.

An Example of Cyber-Attack:

Well, back in **WannaCry, 2017**. More widely known as the first ‘ransom worm’, WannaCry targeted computers running the Microsoft Windows operating system and demanded ransom payments in the Bitcoin cryptocurrency. In only one day, the worm infected over 230,000 computers across 150 countries.

How it started?



Cybersecurity’s history began with a research project during the 1970s, on what was then known as the ARPANET (The Advanced Research Projects Agency Network). A researcher named Bob Thomas created a computer program which was able to move ARPANET’s network, leaving a small trail wherever it went. He named the program ‘CREEPER’, because of the printed message that was left when travelling across the network: ‘I’M THE CREEPER: CATCH ME IF YOU CAN’.

Ray Tomlinson – the man who invented email – later designed a program which took CREEPER to the next level, making it self-replicating and the first ever computer worm. Fortunately, he then wrote another program called Reaper which chased CREEPER and deleted it, providing the first example of antivirus software.

Thomas and Tomlinson’s programs may have been designed as a bit of a mess-around, but they actually served a highly important purpose, revealing a number of flaws in ARPANET’s

networksecurity. This was a huge concern at the time, as many large organisations and governments were linking their computers via the telephone lines to create their own networks. Certain groups of people began to recognise this as well, seeking out ways to infiltrate these lines and steal important data. Say hello to the world's first hackers.

In 1980's the Internet gone mad over the years that followed, computers started to become more and more connected, computer viruses became more advanced, and information security systems could not keep up with the constant barrage of innovative hacking approaches.

The Russians, for example, began using cyber-power as a weapon and, in 1986, employed German computer hacker Marcus Hess to steal US military secrets. He hacked into over 400military computers, including mainframes at the Pentagon, and intended selling their secrets to the KGB. Fortunately, he was thwarted.

Two years later, in 1988, saw the birth of the Morris Worm – one of the major turning points in the history of information security. Network usage began to expand rapidly, and more and more universities, militaries and governments became connected to it. That meant that the security measures required had to gradually become more expansive as well, which gave birth to the Morris Worm.

Named after its inventor Robert Morris, the worm was designed to propagate across networks, infiltrate terminals using a known bug, and then copy itself. Its aim was to identify lacking areas in a network intrusion prevention system.

However, its ability to self-replicate would be its downfall, as the worm replicated so aggressively that it rendered targeted computers inoperable and slowed the internet down to a crawling pace. It also spread quickly throughout the network, and caused untold damage. In fact, the damage it caused was so severe that Robert Morris became the first person to become successfully charged under the Computer Fraud and Misuse Act. The Computer Emergency Response Team (CERT) was also formed as a result, in order to prevent cyber issues like these happening again.

During the 1980s, the ARPANET network also became more commonly known as the internet, and became available to the public as the worldwide web during 1989.

In the mid 90's cyber hacker steals data from targeted users computer and earn a huge a profit from it by selling the data to their desired buyers, As a result of these type of potential threat ,Information Security and NASA research centre built firewall and several other antiviruses which blocked the hackers from stealing the user's private data and making the internet and computer more secure.

Why cyber-security is a necessity in modern digitally evolving world?

Cyber security is becoming an important aspect of life and the reason behind this kind of attitude is nothing but the development of technical dependence. Nowadays having a computer that is full of personal information in every house is a common thing. It is one of the most important things that are needed to be taken under consideration that with good kinds of threats comes a remedy. The remedy in this case is nothing but the development of cyber security. It is becoming a necessary component of our life because all the data regarding security information, health information, personal information, financial information are stored on the internet. It is a place where the data will stay forever but it is not

that secured until security is provided to it. In this piece of writing detailed information is going to be provided for a better kind of situation analysis and remedy find.

The cyber cells of different countries are active all the time in order to find any kind of issues that are not good for people. In order to have a better kind of analysis of the matter, it is highly necessary for a good kind of understanding of why it is important to have a better secured medium and how they are breached. Breaching needs expert supervision. Most of the cases it is seen that the expert hackers have executed the most dangerous crimes of the world. Most of the cases it is seen that with good intentions they have performed the job. Breaching the security and personal life of a person is a crime and it should never be done. The functionality of the cyber cells comes to enforcement in this section and it is one of the most important parts where your total security lies on someone else whom you never know.



It is highly important to have protection against the enemies because cyber breaching can bring secrets in the world of today. There are many incidents and the celebrities face incidents in a regular manner. Most of the cases it is nothing but a hacking performed by people who like in the shadows. It is important because national security lies in it and it is more essential than any individual of any country. Getting the information leaked on the internet can give many issues to the country from the enemies' side.

Some preventive ways to stay away from getting hacked are:

1. Don't click on links from unknown sources.
2. Don't forget to logout from someone else's computer whenever you login to your email and other accounts.
3. Don't share your personal details like Bank account details, ATM-pin, CVV code, sim-card details or PAN-card details, OTP over cellular phone calls to anyone else.
4. Don't click on emails and messages from unreliable sources.
5. Don't wander around malicious and unsecured webpages and websites.
6. Try to stay away from downloading third party application and signing on online agreements granting permission over your personal data and details.
7. Banks doesn't make any phone calls to you and ask for your personal details over phone.

How to became a "Boon to the digitally emerging era" aside from its necessity?

Well, the cyber cells of different units of different countries are always on alert and on a daily basis, they find many issues that are important for them to deal with. The IT section of any department stays in charge of this and it is a good opportunity for all those who are seeking for jobhere.

The salary per annum is higher in cyber-security companies/organisations compared to other IT organisations is because it has huge responsibilities and every sectors is dependent on Internet and want to grow their establishment throw online marketing and sales so they are at a higher risk of getting cyber-attacked to get out of that trouble they are much more reliable on third-party cyber-security companies to keep their databases safe from getting stolen .Which creates a golden opportunity for those people who are working with these cyber security based companies as well as for those people too who are looking for jobs in cyber security cells for database management ,IT security cell maintenance department and also smooth processing online monetary transactions without the fear of getting robbed online from bank to bank transaction using end-to-end encryption system provided by the cryptographers and hashing technology which keeps a person's bank detail safe during and online transaction .

Companies like **Google, Apple, Microsoft, Yahoo!,IBM,Facebook, Intel** are names of few top hiring companies which hire the most people who have worked in IT cells and expanding their domain in cyber-security and how can we forget about **Defence Research Defence Organisation (DRDO)** our country**India's** own biggest IT cyber cells department which are fighting day& night against cyber-crime.

Abstract

WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.

Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards.

WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure.

WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the WiFi Alliance is to 802.11.

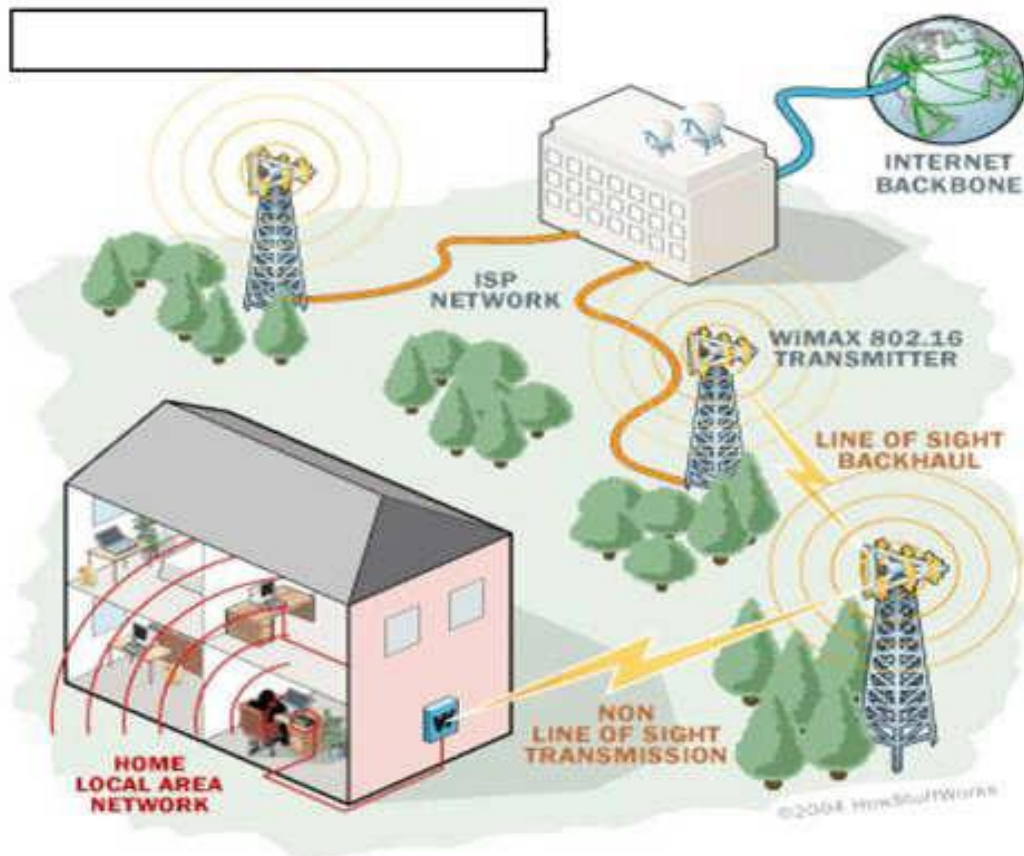
Introduction

WiMAX is-

1. Acronym for **Worldwide Interoperability for Microwave Access**.
2. Based on Wireless MAN technology.
3. A wireless technology optimized for the delivery of IP centric services over a wide area.
4. A scalable wireless platform for constructing alternative and complementary broadband networks.
5. A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models –
 1. A fixed usage model (IEEE 802.16-2004).
 2. A portable usage model (IEEE 802.16e).

WiMAX Speed and Range:

WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.



WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.

With WiMAX, users could really cut free from today's Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a MetroZone.

WiMAX could potentially be deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz

Advantages of WiMAX:

1. WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services.
2. WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.
3. WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.
4. WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and


non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications.

5. WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.

Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

WiMAX & Wi-Fi comparison

Features	WiMAX	Wi-Fi
Primary Application	Broadband Wireless Access	Wireless LAN
Range	A single WiMAX antenna is expected to have a range of up to 40 miles with the speed of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.	Wi-Fi typically provides local network access for a few hundred feet with the speed of up to 54 Mbps
Scalability	WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipment's (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.	Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).
Bit rate	WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.	Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel.
Quality of Service (QoS)	WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. WiMAX provide ubiquitous broadband.	Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS. While, Wi-Fi does not provide ubiquitous broadband
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)
Access Protocol	Request/Grant	CSMA/CA
Half/Full Duplex	Full	Half
IEEE Standards	WiMAX is based on IEEE 802.16.	Wi-Fi is based on IEEE 802.11 standard



Designed by:
Sudeshna Sani
Lecturer, DCST,
Technique Polytechnic Institute,
Hooghly