CHAPTER 1

INTRODUCTION

1.1 HISTORICAL BACKGROUND

“Technology has advanced more in the last thirty years than in the previous two thousand. The exponential increase in advancement will only continue.”

The process of technological advancement is perpetual as has been quoted in above lines by Niels Bohr [1]. Today we live in an age where technology has helped us in developing such communication systems that can practically communicate any sort of information from one end of the world to any corner. However, this stage has not come into existence straight away, rather it has come up on account of number of magnificent advancements, which took place one after another, thereby changing the way we think and live.

Communication has always been the necessity of mankind since its inception. Although several animal species have perfected a system of communication, but humans have been the only species that are capable of developing an effective communication system. Apart from communicating, this system is a vital tool for creating a sense of social cohesion. The history of communication dates back to prehistory where different forms of symbols
were developed and were used in primitive cave paintings and sign language. The oldest known cave painting is that of the Chauvet Cave, dating to around 30,000 BC [2-3] where pigments of fruits, coloured minerals or animal blood were utilised in creating depictions of primitive life on the cave walls.

These were followed by ideograms and pictograms as the next phase of communication media. Pictography is a form of photo-writing whereby ideas are transmitted through drawings and were used by various ancient cultures all over the world since around 9000 BC. Ideograms, through various symbols, messages carved on stone, were used as an efficient means of communication that were able to pass messages for years, but were inefficient in terms of transfer of messages over space. Since such messages could be passed only to certain recipients, so the need was to move the message physically for which a medium, such as a paper was required; on which the message can be imprinted.

Thus for ancient writings, that were generally logographic or alphabetic, first pure alphabets (properly, "abjads") emerged around 2000 BC in ancient Egypt. Here, the only way to increase the speed of communication was to improve the speed of messenger which was decided by good roads, fast riders and well provisioned staging posts where fresh men and horses could be provided. The network of messengers, equipped with horses, emerged as a steady and reliable means of communication. This was further improved by replacing messengers and horses with domesticated pigeons which used to fly straight to the desired destination and so a rapid one-way postal service became possible. This system of passing information was quiet useful and efficient and was utilised by various emperors including Genghis Khan, one of the swiftest and most wide-ranging conqueror of medieval history who utilized this system to send information of each new conquest to his homeland in Mongolia. Thus writing messages became popular which led to the development of handwritten books and documents
and were followed with the development of a formal postal system. The
renaisance of communication had thus begun and this marked the
commencement of development of information in various parts of the world.
The next challenge in front of mankind was to develop more information and
to pass it to another place. Passing the information to a physically distant
place is usually termed as “telecommunication”.

1.1.1 Development of Telecommunication

Although the history of telecommunication incepted with the use of
smoke signals and drums in various regions of Africa, America and Asia, in
1792, a French engineer, Claude Chappe formed the first visual telegraphy
(or semaphore) system in France, between Lille and Paris. Experiment in
electrical telegraphy, an 'electrochemical' telegraph, was demonstrated in
1809 by a German physician named Samuel Thomas. The first commercial
electrical telegraph was developed in 1839 by Sir Charles Wheatstone and
Sir William Fothergill Cooke in England where the deflection of needles was
used to represent messages and was operated over a distance of about 21
kilometers. Based on this, first commercial telephone services were set up in
1878 by Alexander Graham Bell that grew quickly in every major city of the
United States by mid-1880s.

In the start of 20th century, a new form of communication called radio
communication came into picture. It was first used as short-wave
communication during World War-1 and blossomed into the most popular
communication and entertainment technology of the era after the war was
over. Until 1925, approximately 2 million homes had radios and there were
several hundred stations broadcasting thousands of programs. Frequency-
modulated radio made its first debut in 1933 when Edwin Armstrong, "the
father of FM radio", invented it. After the invention of Television in 1939,
when radio was one of the favourite form of communication among the
masses, with the continuous development of IC technology, people have
started adopting the television as a major source of communication. Thereafter a phenomenal advancement which could be stated as a big tool for modern day communication systems was the development of first electronic computer. With this, the Internet marked the start of new era in the field of communication where a group of computers for military purposes were connected to each other for sharing of information through emails and websites. Soon the internet started catching on and firstly it was adopted by corporations and then slowly the internet became ubiquitous, faster, and increasingly accessible to non-technical communities which led to its use for number of other applications. It was widely accepted and used by households, companies, schools, organizations, business houses for socializing, conducting research, and advertising. With the advent of cell phones the mobile communication started. These have started becoming one of the most important components of development indices. As per ICT facts, globally mobile-cellular subscriptions have enhanced enormously from 962 million to 5972 million during last one decade [4]. The customer base has expanded from 15.5% to 85.7% of the world inhabitants using this device during last one decade (Fig. 1.1).

![Global mobile-cellular subscriptions, total and per 100 inhabitants, 2001-2011](image)

**Figure 1.1: Global mobile-cellular subscriptions, 2001-2011**
It was also observed that the growth in mobile-cellular subscriptions is not just limited to the level of development of nations (Fig. 1.2), as in the year 2000, out of 719 million subscriptions; 469 million were in developed countries whereas developing countries contributed only 250 million subscriptions. In 2005, there were 1215 million subscriptions in developing countries par exceed that of developed countries (992 million) and the trend continues, like in year 2011; it is nearly 2.8 times over the developed countries.

**Figure 1.2: Mobile-cellular subscriptions, by level of development**

### 1.2 LATEST ADVANCEMENTS IN COMMUNICATION

The modern world is equipped with a large number of advanced communication technologies and systems. Laptop or a portable computer has been explored as an integral utility tool in telecommunication. With latest terms like “smart phone” coming up, which stands for a hybrid device between smart phone and laptop, every person in the society is after a fast, reliable and efficient communication system. Now various communication devices have been continuously developing in form of laptops, netbooks, smart phones, ipads so as to bridge the gap between various communications systems, to pass the information from one type of the device to another and
from one type of technology to the other. As per ITU World Telecommunication /ICT Indicators database reports of 2012, more than 85% of the world population presently depends on cellular mobile systems. The region wise distribution during last decade among the world has been depicted through Fig. 1.3.

**Figure 1.3: Mobile-cellular subscriptions, per 100 inhabitants, 2011**

With such vivid communication system in use, the mode of transfer of information in any form of text, audio or video started getting more and more popular. Major application areas of these devices and technologies are in homes, offices and public hot spots where wireless communication comes to picture. Wireless communication is the technique of transferring information through a distance without the use of wires or electrical conductors. Some of the latest wireless devices are mobile phones, two way radios, personal digital assistance (also known as a PDA), wireless networks, GPS unit in cars, satellite television and other electrical equipment. Wireless communication has helped latest technology to reach to, new levels of
communication heights. Wireless has truly become the window for future communication. Wi-Fi is a wireless networking technology that allows computers, mobile phones, ipads, game consoles, and other utility devices to communicate over a wireless signal. WiFi (or Wi-Fi) is short form for Wireless Fidelity. Vic Hayes is known to be the "father of Wi-Fi technology" because he chaired the IEEE committee that established the 802.11 standard in 1997 to make Wi-Fi feasible. Thereafter, improvements to the network bandwidth were added to the basic 802.11 standard. With the development of more and more sophisticated communication systems we are in a stage where number of devices such as laptops, notebooks, printers, wired LANs, internet, wireless LANs, PDAs, mobile phones etc. are utilising this WiFi technology. Thus the processed data which is mobile in various systems and devices is usually known as “Information”. Today information forms an important part of our daily routine and this era is popularly termed as the “Era of Information Technology”.

1.3 INFORMATION

Today, world-over, the “Information” is assumed to be a vital asset to any organisation or an individual as it plays an important role in almost every sphere of life. Information is available in various forms such as literature in books, findings of a scientist, experimental data, scheduling records, paintings, financial accounts, product specifications, staffing lists, technical communication, data available within military information systems and recordings in ledgers of an organisation [5-6]. Since there is a wide spectrum over which the information types are distributed, a system is required for management, dissemination, classification and presentation. Such a system may be a collection of hardware, software, data, people or procedures that are designed to perform various information related activities that support the day-to-day, short-range, and long-range activities of users in an organization. With modern communication technology, information
Introduction

dissemination has become cheaper, quicker, and more efficient. We can now communicate with anyone around the globe simply using text message, email, video conferencing or by any other means. Thus modelling, building, maintenance and management of information and information systems has arisen [7-11]. The type of information and the system for its processing and dissemination varies from one form to another. In general, an information system is a system which provides facilities like the storage, retrieval, connection, and evaluation of information. Different types of information systems are as under:-

1.3.1 Home and Office Information System

A home and office information system utilizes hardware, software and networks to enhance work flow and makes communication feasible among users. In this information system, the users perform various tasks with the help of various electronic devices and computers. Such an information system allows the information to be shared among its users and outside world through some communication channel. Home and office information systems use communication technologies such as voice mail, facsimile (fax), videoconferencing, and electronic data interchange (EDI) for the electronic exchange of text, graphics, audio, and video. This information system also uses a variety of hardware, including computers equipped with modems, video cameras, speakers, microphones, scanners and fax machines. An office information system supports a range of business office activities such as creating and distributing graphics and/or documents, sending messages, scheduling, and accounting. A similar counterpart at home supports exchange and processing of personal data. Various applications in home as well as office information system include spreadsheets, databases, presentations, graphics, e-mail; activities like word processing, web browsing, web page authoring, personal information management, and groupware.
1.3.2 Transaction Processing Systems

An information system which processes data generated during transactions such as a deposit, payment, order or reservation of an organisation is known as a Transaction Processing System (TPS). Transaction processing systems may include recording of an activity, confirming some business action, generation of a response as well as data maintenance and handling. Urge to convert manual system to computerized system has led to development of computerised TPS which allows faster processing and reduction in overall cost. TPS also provides system runtime functions, by providing execution environment ensuring with better integrity, availability and security. With better computational capabilities and development of internet Online Transaction Processing (OLTP) too has gained popularity. Such systems enhance capacity as well as efficiency of a TPS on account of which reliability and applications of TPS have enhanced tremendously.

1.3.3 Tele-medical Information Systems

Our world is changing from an industrial to an information and telecommunication society. In the field of medicine, large amount of information is required to be stored and retrieved which includes clinical data, clinical decision making, therapeutic data, inventory control, billing, finance and budgets, administration and patient care. Information systems which provide these facilities are called Tele-medical information systems (TIS’s). TIS’s form the basis for telemedicine services as well as for health information services [12]. In recent years, rapid advances in information integration methods have spurred tremendous growth in the use of integrated information systems in healthcare delivery [13, 14]. The TIS helps in recording key information at the point of health care so as to eliminate duplication of data storage and data entry thereby ensuring that data are accurate and complete. This information system facilitates clinical decision
support that enables healthcare providers to take better informed decisions by ensuring confidentiality and security of patient records. It can thus be used to help patients manage their own health thereby providing reliable performance. It is used to automate processes and facilitate sharing of information, which helps to save time for the entire medical team.

1.3.4 Management Information Systems

These information systems help in decision making, taking reports and analysing the outcomes of TPS. Thus input to management information system (MIS) is provided by the transaction processing information systems. A MIS provides several benefits to the organization by providing effective and efficient means of coordination between various departments, quick references, speeding information seeking and improving general organisation [5]. It further facilitates an easy access to relevant data as well as documents; and reduces labour and manages day to day activities in an organisation [15-16]. For example, when sales data information of any organisation are provided by TPS, it becomes luring for the managers to use data to track records, supervise, solve difficult problems and to arrive at the final decision. Thus MIS produces an accurate, more meaningful and ordered information. MIS provides an option to provide detailed information with complete analysis or an abstract type of information for quick reference.

1.3.5 Decision Support Systems

Decision Support Systems (DSS) are a particular class of information systems, designed to help users to reach a particular decision, generally using some software, when a decision-making situation arises. This class of information system supports business and organizational decision-making activities. A DSS is an interactive system, intended to help decision makers, to compile functional information from unprocessed data, documents, personal knowledge, and/or business models; to identify and solve problems
so as to take a definite decision. A decision support system may be used to provide a comparative analysis of different decisions, based on factual data being provided by TPS. It may be noted that TPS and MIS are used on a regular basis in an organization, while DSS are specifically developed for taking appropriate decisions only. It may be used to calculate projected sales, to launch new products and other productive decisions based on the requirements of an organization through spread sheets and databases.

1.3.6 Integrated Information Systems

With advances in communication and computing devices, a single system may be used for vast number of applications. Such a system is called an integrated information system. Organisations are increasingly becoming dependent on software which processes transactions and is also capable of decision making by generating management information reports [13, 17-18]. Such systems increase the overall capability of the information systems.

1.4 GROWTH OF INFORMATION NETWORKS

Information networks, also known as computer networks, are growing rapidly since last few decades. These networks use data transfer on different forms of transmission media. While data is available on transmission media, it is vulnerable to eavesdropping as well as attacks. Thus reliability and authenticity of the network is challenged. Hence the need of security in computer networks arises. The reasons to protect the information on our computer systems are:-

- Security in computer network ensures that information remains confidential and is accessible only to authorized users.

- Integrity of the system enhances as it leads to the development of confidence among users that information is not prey to change by unauthorized users.

- Helps in risk measurement and management during urgencies [19-21].
Although information security can be dated back to early 1990’s, the recent increase in network security attacks, viruses, worms as well as Trojans have brought the security of computer networks to the central platform in today’s world and so a modern network is vulnerable to a diverse variety of attacks. Real-time applications like railway signaling control systems and medical electronics systems are increasing in the modern world which requires high quality of security to ensure confidentiality and integrity of information. Therefore, it is not only desirable but essential also to fulfill security requirements in security-critical real-time systems. The recent years have witnessed an increase in research interest for analysis of security in virtual and real time performances [20, 22-25]. But despite the best efforts put in by various agencies, industries and associations, they are not confident enough about the complete security of a network.

The use of internet has enhanced the requirement of information networks. Although the initial objective to use internet was to allow people to communicate with each other in different forms but now it is coming up with a diverse range of applications. Internet is no longer just about e-mail or surfing Web sites, in fact, it has emerged as a vital medium to search, access various databases, reach customers, find commercial commodities, share views and enhance a business. It empowers the business activities using e-commerce and provides customers an easily accessible medium for shopping different commodities. The internet is used in different spheres of life. It has eased the conferencing, information sharing, banking facilities, library utilities and booking agencies.

Internet facilitates the users an easy and suitable means of communication in the form of emails and live chatting facilities. Online communication increases the accuracy thereby almost eliminating the time of delivery of message. The facility of audio-video conferencing in Internet allows a group of users, being located at different distant places to communicate with each other as if they are sitting in a single room. In the
field of medicine, doctors can discuss typical cases without actually visiting the patient with different specializations. Engineers and scientists can depict their latest research findings that can be beneficial for other researchers and academicians who might be in far-off laboratories. Similarly the Internet has given a new means to shopping of different products or services around the world. Web has provided a big platform even for various artists and philosophers to share their ideas thereby reaching a greater number of followers throughout the globe. Advertising is another avenue where internet has helped in the promotion of various products among large number of people at a reasonable cost. With increase in number of internet users, this mode of advertising is attractive and also helps reach the customer in a better way. Various examinations, online bookings and registrations are internet based so as to manage the large amount of data generated. Number of software are used throughout the world which can be developed, distributed, authenticated and shared easily with use of internet.

Due to the applications offered by internet, a larger portion of population throughout the globe has started falling for it. The increase in internet penetration in society can be judged from Table 1.1 and Fig. 1.4 where four countries have been taken into consideration. This clearly depicts that there has been an exponential increase in percentage of individuals using internet in all countries in last few years.
Table 1.1: Percentage of Individuals using the Internet in different countries of the World [4]

<table>
<thead>
<tr>
<th>Year</th>
<th>India</th>
<th>China</th>
<th>United Kingdom</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>0.53</td>
<td>1.78</td>
<td>26.82</td>
<td>43.08</td>
</tr>
<tr>
<td>2001</td>
<td>0.66</td>
<td>2.64</td>
<td>33.48</td>
<td>49.08</td>
</tr>
<tr>
<td>2002</td>
<td>1.54</td>
<td>4.60</td>
<td>56.48</td>
<td>58.79</td>
</tr>
<tr>
<td>2003</td>
<td>1.69</td>
<td>6.20</td>
<td>64.82</td>
<td>61.70</td>
</tr>
<tr>
<td>2004</td>
<td>1.98</td>
<td>7.30</td>
<td>65.61</td>
<td>64.76</td>
</tr>
<tr>
<td>2005</td>
<td>2.39</td>
<td>8.52</td>
<td>70.00</td>
<td>67.97</td>
</tr>
<tr>
<td>2006</td>
<td>2.81</td>
<td>10.52</td>
<td>68.82</td>
<td>68.93</td>
</tr>
<tr>
<td>2007</td>
<td>3.95</td>
<td>16.00</td>
<td>75.09</td>
<td>75.00</td>
</tr>
<tr>
<td>2008</td>
<td>4.38</td>
<td>22.60</td>
<td>78.39</td>
<td>74.00</td>
</tr>
<tr>
<td>2009</td>
<td>5.12</td>
<td>28.90</td>
<td>78.00</td>
<td>71.00</td>
</tr>
<tr>
<td>2010</td>
<td>7.50</td>
<td>34.30</td>
<td>78.00</td>
<td>74.00</td>
</tr>
<tr>
<td>2011</td>
<td>10.07</td>
<td>38.30</td>
<td>82.00</td>
<td>77.86</td>
</tr>
</tbody>
</table>

Figure 1.4: Percentage of individuals using the Internet
The growth of internet use is observed in both developed as well as developing countries. The percentage of households with Internet access has been increasing in both in developed as well as developing countries (Fig. 1.5).

![Percentage of households with Internet access by level of development, 2002-2010](image)

*Figure 1.5: Percentage of households with Internet access by level of development, 2002-2010*

It has further been observed that the number of internet users as well as percentage of population using this technology has been globally increasing every year (from 495 million in year 2001 to 2,265 million in year 2011) (Fig. 1.6).
Based on the type of interconnection between various network components, the information networks for electronic information communication can be broadly classified as wired networks and wireless networks.

### 1.5 WIRED NETWORK

Wired network is used for such applications that require connections for fixed computational facilities. In this network, computer and other appliances such as fax machine, printers are connected to each other using a physical transmission medium such as coaxial cable, optical fibre cable or even copper conductor wire. In wired networking, cables run across the complete building from one computer to another carrying the information signals. The type and extent of wiring depends on a number of factors, such as topology used, size of building premises and number of nodes in the network. A wired network comprises Ethernet cables, switches and routers.
A wired network uses a number of wires for providing links between various network devices converting even a small network complex. Fig. 1.7 shows a typical wired LAN with few number of devices connected together to share common resources.

![Figure 1.7: Typical Wired LAN](image)

Fixed telephone network and fixed broadband networks are common examples of wired networks. During last decade, the trend in telephone subscriptions has been depicted in Fig. 1.8 and fixed (wired)-broadband subscriptions have been depicted in Fig. 1.9. Although the interest in fixed telephone has more or less saturated in comparison with the trend of fixed broadband subscriptions.
Figure 1.8: Fixed-telephone subscriptions per 100 inhabitants, 2001-2011

Figure 1.9: Fixed (wired)-broadband subscriptions per 100 inhabitants, 2001-2011
Similarly, the numbers of inhabitants per 100 having subscribed to fixed broadband wired network in different continents of the world as in recent years have been observed as shown in Fig. 1.10.

![Fixed (wired)-broadband subscriptions per 100 inhabitants, 2011](image)

* Commonwealth of Independent States

Regions are based on the ITU BDT Regions, see: [http://www.itu.int/ITU-D/ict/definitions/regions/index.html](http://www.itu.int/ITU-D/ict/definitions/regions/index.html)

Source: ITU World Telecommunication /ICT Indicators database

**Figure 1.10: Fixed (wired)-broadband subscriptions per 100 inhabitants, 2011**

### 1.6 WIRELESS NETWORK

Wireless network refers to a network which does not involve the use of cables. Wireless communication is known to be the window for future networking which eliminates the use of electrical cord. This technology has permitted us to expand our horizons in communication beyond what we thought would be possible. This technique has helped entrepreneurs, telecommunication engineers and network administrators to save the cost of cables for networking in specific premises in their installations. Wireless communication uses electromagnetic waves for implementation, administration and data transfer such as radio frequency, infra red light, laser
light or acoustic energy. The term wireless is not the same as cordless. Cordless is where powered electrical devices are able to operate from a portable power source and has a limited range but a wireless device has a comparatively larger range. From a simple TV remote to satellite links, wireless communication finds application in wide areas including cellular phones and modems. This technology has become increasingly popular in last few decades. It was observed that the percentage of global mobile subscription has increased from 15.5 % in 2001 to 85.7 % in the last couple of years.

Wireless networks are poised to play a vital role in the communication networks of future on account of its freedom from the restriction of wires. Some of the other benefits of a wireless network include easier setup, hassle free connections, ease of installation with no drilling and cabling requirements. Moreover it saves time and botheration when physical places are shifted very often in addition to an easy expansion of the network. These networks allow use of laptops anywhere within a region from home to office and thus provide the facilities like, surfing internet, printing, file transfer and many more applications. The development of wireless networks is still in progress as the usage is rapidly growing. Personal communications are made easy with the advent of cell phones where radio satellites are used for networking between continents. Whether small or big, businesses uses wireless networks for fast data sharing with economical means. Sometimes compatibility issues with new devices might arise in these extremely vulnerable networks but the technology has made the uploading and the downloading of huge data a piece of cake with least maintenance cost.
Since wireless networks use radio waves, a number of devices, hereby called *nodes*, can be connected to it without increasing the complexity. Fig. 1.11 depicts a typical wireless LAN with number of nodes connected together. Laptops and other wireless computing devices can be stirred around freely within a wireless network because mobility of wireless network is superior as compared to wired networks. WLAN is the most common form of a wireless network usually found in university campuses, hot spots, public buildings and hotels to provide internet facility to clients when they are in mobile mode. Nevertheless a wireless network depends on wireless devices, access points, adapters and WLAN cards for its operation but these devices are comparably of higher cost. Thus the initial set-up cost for a wireless network is more than a wired network. Even reliability of a wireless network is less as compared to a wired network. These networks are not limited to physical boundaries and, therefore, are vulnerable to various attacks. With increase in the use and deployment of these networks, the need to protect them from various attacks has become a prime concern.
Wireless network can be set-up in two ways depending on how the network nodes are communicating with each other, specifically infrastructure mode or ad-hoc mode. The ad-hoc mode is also called peer-to-peer mode. In the infrastructure mode the devices in a wireless network are made to communicate either indirectly through a central point known as an access point, whereas in the ad-hoc mode the nodes communicate directly, one to the other. An ad-hoc network also called Wi-Fi Direct network is a network where stations communicate only peer to peer (P2P). This mode comprises of wireless network adapters that are able to automatically locate and communicate with each other. This is a cost effective technique of setting up a wireless network and acceptable for a network that consists of small number of nodes. However, there are limitations on the size and topology of the network used. This mode of wireless network becomes difficult to implement when the size of the network grows. This difficulty arises due to the fact that if some of the intermediate nodes stop working, many of its functionalities are lost. Since ad-hoc wireless network supports mobility, it suffers considerably while connectivity is lost as and when the nodes get out of range.

Howbeit, the infrastructure mode, overcomes the obstacles experienced using the ad-hoc mode, it requires the use of wireless access points which, expectedly, adds to the cost of implementing a wireless networking solution. Another advantage which is offered by the infrastructure mode is robustness. These networks provide a bridge network between wireless and wired installations and increase the reliability of overall network. Another advantage offered by this wireless network type is expandability. Access points used in these networks allow easy expansion as and when need arises.

Following are the key features which differentiate an ad hoc mode wireless network from infrastructure mode
• The Infrastructure mode wireless network can be used for a wider range as it uses an access point which works on higher power. On the other hand, range of ad hoc mode connections is limited by the power of the network devices.

• Ad hoc mode does not require an access point thereby making configuration easier and useful especially in applications where network layout involves frequent changes.

• The physical parameters associated with an ad hoc mode wireless network change dynamically and may cause variations in the behaviour of a network.

Although number of wired networks has increased steadily, in recent years, we have witnessed an increase in the interest of users towards wireless networks also [4, 20]. As per ITU World Telecommunication /ICT Indicators database reports, 2012 percentage of world population using fixed broadband has increased from 20.6% to 34.7% over last 4-5 years whereas in case of mobile broadband it has increased from 4.0% to 15.7% thus marking an enhancement of 3.9 times as compared to 1.7 times rise for fixed broadband [4]. The field of wireless network systems has grown tremendously in past few years causing it to become one of the fastest growing segments of the telecommunications technology. As wireless networks evolve with increasing size and profitability, they are able to integrate with other wireless technologies enabling them to support various applications such as mobile computing and mobile communication and perform as efficient as wired networks. One of the most important features that a wireless network such as 802.11 wireless local area networks (wireless LAN) brought to organizations is the omnipresent access to information. By providing unbounded and mobile connections to corporate network, these networks allow people to reach the critical information anywhere within the office locality and thus can potentially increase the efficiency and the
competence in the business community up to 22 percent [26-27]. Due to the difficulties posed by the wireless transmission medium and increasing demand for better and cheaper services, the field of wireless networks has become an area of research and development. The fast growth of wireless systems in recent years, together with the exponential growth of the Internet is increasing the demand for wireless data services and devices for which complete analysis is still required to be carried out [28-29]. Since a wireless network can support a variety of applications, the traffic on upcoming wireless systems is a mix of real-time traffic such as multimedia teleconferencing, real time voice, and data-traffic such as internet browsing and file-transfers, with users desiring diverse Quality of Service (QoS). Such a range of data makes the data on the wireless network vulnerable to a number of attacks. Guaranteeing the QoS for these traffic types and providing security from various attacks is considered a great challenge and on-going research activity. Wireless networks are also used in vehicles as Secure Wireless Personal Area Network (SWPAN) [30]. Novel schemes have been introduced for wireless connectivity and development of new business models using low cost wireless LAN equipment which operate in unlicensed spectrum. This has completely revolutionized local area communications, and led to the development of new home and office networking models. The ease of deployment of Wi-Fi has made it ubiquitous in densely populated urban areas, which has led to the emergence of various wireless community networks. Within a short span, wireless communities started using inexpensive wireless technology to communicate that led to the development of autonomous wireless internetworks, thereby offering a variety of broadband services. Wireless Community Networks (WCNs) have been developed as preliminary movements of WLAN enthusiasts, who use economical networking equipment for free interconnection and the unlicensed frequency band thus forming all-wireless autonomous networks [31]. The wireless networks have been well adapted and number of wireless devices along with number of people using them is increasing day by day.
As indicated in Fig. 1.12, the number of mobile broadband subscribers per 100 inhabitants has increased from 0.8 to 8 in last 4-5 years indicating an increase of nearly 10 times for developing countries. On the other hand in developed countries the number per 100 habitants has increased to 51.3 from 18.5, marking an increase of 2.7 times. For whole of the world, increase in this number is about 4 times. As observed from Fig. 1.12 and Fig. 1.13 the number of mobile broadband users per 100 is more in developed countries, but its popularity is increasing at a very fast pace in the developing countries too.

Figure 1.12: Comparison of active mobile-broadband subscriptions per 100 inhabitants for developed and developing countries.
Figure 1.13: Active mobile-broadband subscriptions per 100 inhabitants, 2011

1.7 WIRED VERSUS WIRELESS COMMUNICATION

As discussed above, there are two broad categories in which a computer network may be classified, namely, wired networks and wireless networks. A local area network used generally in homes and offices using some data transfer physical channel such as coaxial cable is classified as a wired network. Common examples of wired LANs include Ethernet or wired LAN. A wired LAN uses Ethernet cables, network adapters and switches. Although two computers may be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or routers to accommodate more computers. On the other hand wireless network is the type of computer networking in which computer is connected with different telecommunication devices wirelessly. Although both wired and wireless can claim advantages over the other; both
represent viable options for home and other local area networks (LANs). Traditionally wired LANs have been used for domestic as well as office use, but wireless technologies are gaining popularity at a very prompt pace. Wireless technologies are designed to reduce installation time and obviate the users from different types of obstacles produced by the cabling. Therefore, wireless networks grant more convenient working as compared to other type of wired networking.

Establishing a wired LAN is tougher as it requires Ethernet cables which run under the floor or through walls, especially when LAN is spread over different portions of the building. These hardware constraints encountered during installation make a wired LAN more difficult to install. Different configurations of networking are employed while installing a wired LAN which depends on type of devices, type of internet connections used and the type of application it is intended for. Although wired or wireless LANs do not diverge much with respect to configuring as both rely on standard Internet Protocol and network operating system configuration options. However, use of an access point in a wireless network tends to make overall installation easy in wireless LANs as it avoids the need of complex cabling and thus its excessive maintenance.

We also need to spend more time in configuring or setting-up the wired home network as it requires spreading a network of coaxial cables while it is easy to setup the wireless networking devices and that too at a reasonable cost. In wired networks, the various accessories viz., Ethernet cables, hubs, switches etc; are less costly than wireless accessories. Nevertheless, overall cost of a wireless network reduces due to the ease of installation involved.

1.8 NETWORKING PROTOCOLS AND MODELS

In general, protocol is a set of rules used by end points in a telecommunication system during the process of communication, thereby
specifying the interactions between communicating entities. Thus a network protocol is a set of rules that governs communication between different nodes in a network. These rules include guidelines that regulate characteristics of a network such as access method, allowed physical topologies, types of cabling, and speed of data transfer. Transmission Control Protocol/Internet Protocol (TCP/IP) and the OSI reference model are some of the most popular collection of network protocols. The TCP handles the reliable delivery of the message of different sizes. On the other hand, the Internet Protocol manages the routing of network transmissions from the sender to receiver. Although TCP/IP and OSI form only a small fraction of total collection of protocols developed so far, these two are responsible for ferrying the major bulk of data across the Internet, as these are the most commonly used protocols [32-33].

1.8.1 OSI reference model

Governed by ISO standard 7498, the ISO/OSI network reference model was developed as a part of an international standards initiative in 1980’s that was supposed to be an usher in a new and improved suite of protocols. This model provides a layered approach which breaks the networking into seven layers. The seven layers combined together are often referred to as a "Network Stack." The OSI model provides only the guidelines as to how the computers should communicate over a network but not the procedures or protocols.
The seven layers of the OSI Reference Model named from top to bottom, can be illustrated as in Fig. 1.14 (a):

<table>
<thead>
<tr>
<th>OSI 7 layer reference model</th>
<th>Internet Protocol Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>FTP, Telenet, SMTP, SNMP</td>
</tr>
<tr>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Transport</td>
<td>IP</td>
</tr>
<tr>
<td>Network</td>
<td>ARP, RARP</td>
</tr>
<tr>
<td>Data Link</td>
<td>Not Specified</td>
</tr>
<tr>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1.14: Mapping of Internet protocol suite and corresponding OSI layers

1.8.1.1 Application Layer/Layer 7

It enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. It specifies network-related functions for a user application or program to ensure that communication with another application over a network is possible. It's important to note that this is not the user interface itself. User's software programs interact with the Application Layer.
1.8.1.2 Presentation Layer/Layer 6

It accepts the data from an Application Layer and converts or encodes it into a standard format that an Application Layer can understand on the other computer. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

1.8.1.3 Session Layer/Layer 5

This layer establishes, manages, and ends the connections or sessions between the applications on the communicating computers. It also maintains and synchronizes the interaction among communicating systems.

1.8.1.4 Transport Layer/Layer 4

The purpose of transport layer is process-to-process delivery of the entire message where a process is an application program, running on a host. This layer accepts data from the upper layer, converts it into a format that can be transmitted over the network, and manages the flow of data between the two hosts that are communicating.

1.8.1.5 Network Layer/Layer 3

The network layer is for source-to-destination delivery of a packet, possibly across multiple networks, while it receives a segment from Layer 4, it adds a header to it to create a "packet," and then sends the packet to Layer 2. Here the role of Layer 3 is to deliver the packet to the destination computer. If there is more than one route to the destination computer, the Network Layer chooses the best path in accepting the packet while treating each packet as an independent one.
1.8.1.6 Data Link Layer/Layer 2

This layer receives packets from Layer 3 and adds another header to form a "frame." The Data Link Layer can also add a trailer to the frame, such as a Cyclic Redundancy Check (CRC). Finally, the Data Link Layer translates the frame into binary digits, or bits, for Layer 1. Thus the data link layer divides the stream of bits received from the network layer into manageable data units called frames. Other functions of the data link layer are physical addressing, flow control, error control and access control.

1.8.1.7 Physical Layer/Layer 1

The physical layer coordinates the functions of carrying a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. Layer 1 defines the electrical or optical signal that equals either a one, or a zero. Physical Layer standards include cabling specifications, electrical or optical signalling, and lower-level framing of 1’s and 0’s.

As the data moves down the OSI layers, the data is encapsulated in headers and possibly trailers/footers at each layer. When a lower level receives the information, it treats the entire package as data. At the receiving end, each layer examines and removes its corresponding header and trailer/footer.

1.8.2 TCP/IP

TCP/IP was initially designed to meet the data communication needs of the Department of Defense (DOD) of U.S.A. In late 60s, the Advanced Research Projects Agency (ARPA, now called DARPA) of Department of Defense (U.S.A), initiated a partnership with universities and corporate research community of U.S.A for the design of an open standard-protocol for multi-vendor networks and the first packet switching network named
ARPANET was suggested. In 1969 the first experimental four-node version of ARPANET was successfully launched that ultimately evolved into a useful operational network, the "ARPA Internet". In 1974, the design for a new set of core protocols, for ARPANET, was proposed by Vinton G. Cerf and Robert E. Kahn and it was named as Transmission Control Protocol/Internet Protocol Suite, commonly referred to as TCP/IP.

The TCP/IP reference model is thus a simpler, four-layer model defining specific protocols at each layer. The four layers in TCP/IP are:-

1.8.2.1 Application Layer

This layer has not only the functionality as in the case of Application Layer in the OSI model, but it also manages the encoding, data compression, encryption, and sessions.

1.8.2.2 Transport Layer

It has the same functionality as has been in the Transport Layer in the OSI model. It defines the level of service and status of the connection used while transporting data.

1.8.2.3 Internet Layer

This has again the same functionality as of the Network Layer in the OSI model. It converts package data into IP datagrams, which contain information about source and destination address and is used to perform routing.

1.8.2.4 Network Access Layer

It mainly focuses on how data is to be transmitted over any type of the physical medium, such as coaxial cable, optical fibre, or twisted-pair copper wire on a network, like LAN or WAN. It specifies the details of how data is
physically sent through the network and how bits are electrically signalled by hardware devices that interface with network.

1.8.3 Five-Layer Model

This model is a combination of the OSI and TCP/IP reference model consisting of 5 layers. Here Network Access Layer is partitioned in such a way that both the Physical Layer and the Data Link Layers could be included and the layers are:

- Application Layer/Layer 5
- Transport Layer/Layer 4
- Network Layer/Layer 3
- Data Link Layer/Layer 2
- Physical Layer/Layer 1

1.8.3.1 Application Layer

Application Layer protocols specify the details of encoding, compressing, or encryption of data and also as to how the sessions should be managed. This layer includes popular protocols like HTTP, FTP, DNS and SMTP.

1.8.3.2 Transport Layer

The Transport Layer provides an end-to-end service to applications running on end hosts. The Transport Layer specifies which Application Layer protocol should be used to process the data on the receiving computer. There are two common transport layer protocols:

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
UDP is a simple and fast "best effort" delivery protocol with features of delivery notification, error checking, or recovery procedures. It is commonly used for short messages and time-sensitive data. UDP allows applications to send datagrams that preserve message boundaries but imposes no rate control or error control. TCP is a robust protocol providing delivery notification, error checking, and recovery procedures. It deals with the problems that are not repaired by the IP layer like packet loss, duplication, and reordering. The receiving computer tells the sending computer when the data was received. TCP operates in a connection-oriented fashion and does not preserve message boundaries. Examples of applications that use TCP are HTTP, SMTP and FTP.

1.8.3.3 Network Layer

The Network Layer (IP) provides an unreliable datagram service and must be implemented by all systems addressable on the Internet. The Network Layer receives data segments from the Transport Layer and adds a header to create a packet. A packet is one unit of data encapsulated at Layer 3. Each packet contains a header followed by the data. The packet's header specifies the data's source and destination IP addresses. Each packet header also specifies the IP protocol number that signifies the upper layer Transport Layer protocol being used. Each Transport Layer protocol is assigned a unique identifier, or IP protocol number.

1.8.3.4 Data Link Layer

The Data Link Layer receives packets and adds its own header to each packet while creating a frame. A frame is one unit of data encapsulated at Layer 2. Each frame is divided into three parts:

- Header
- Data
- Trailer
The header contains source address of data from layer 2 and also its destination address. It indicates which protocol is to be used to process the data at Layer 3, on the receiving node. The frame trailer is a checksum such as CRC, which is used to verify the data integrity. Finally, Layer 2 converts the data into a pattern of 1’s and 0’s.

1.8.3.5 Physical Layer

This layer converts bit pattern into corresponding electrical signals and sends them across the physical medium. Physical Layer specifications define characteristics such as cabling specifications, voltage levels, physical data rates, maximum transmission distances, and physical connectors.

1.8.4 Mapping OSI and IP suite

The Internet protocols are the world’s most popular open-system (non-proprietary) protocol suite as they can be helpful in communicating across any set of interconnected networks and are well suited for both LAN and WAN communications. The Transmission Control Protocol (TCP) and the Internet Protocol (IP) form a part of collection of protocols, commonly known as internet protocols. Fig. 1.14(b) illustrates the mapping of protocols in internet protocol suite with corresponding OSI layers.

1.8.5 802.11 standard

802.11 is a set of standards for implementing wireless local area network (WLAN) communication which are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The standard reserves the low levels of the OSI model namely the physical layer and the data link layer for wireless connections. The physical layer defines the radio wave modulation and signaling characteristics for data transmission, while the data link layer defines the interface between the machine’s bus and the physical layer. The 802.11 standard actually has three types of physical layers depending upon the mode of transmission used viz., Direct Sequence Spread
Spectrum (DSSS), Frequency-hopping spread spectrum (FHSS) and Infrared as shown in Fig. 1.15.

<table>
<thead>
<tr>
<th>Data Link Layer (MAC)</th>
<th>802.2</th>
<th>802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer (PHY)</td>
<td>DSSS</td>
<td>FHSS</td>
</tr>
</tbody>
</table>

**Figure 1.15: 802.11 layers**

The IEEE 802 standards committee defines two separate layers for the Data-Link layer of the OSI model: The Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The specifications defined for the physical layer and the media access control (MAC) layer communicates up to the LLC layer, as shown in the following Fig. 1.16. Any protocol working on a higher layer may be used on a Wi-Fi wireless network in the same way as it is used on an Ethernet network.

<table>
<thead>
<tr>
<th>OSI model</th>
<th>802.2 Logical Link Control (LLC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>802.3</td>
</tr>
<tr>
<td>Presentation</td>
<td>802.4</td>
</tr>
<tr>
<td>Session</td>
<td>802.5</td>
</tr>
<tr>
<td>Transport</td>
<td>802.11</td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td>Ethernet</td>
</tr>
<tr>
<td>MAC</td>
<td>802.3 Token Bus</td>
</tr>
<tr>
<td>Physical</td>
<td>802.4 Token Ring</td>
</tr>
<tr>
<td>Physical</td>
<td>802.5</td>
</tr>
<tr>
<td></td>
<td>802.11 Wireless LAN</td>
</tr>
</tbody>
</table>

**Figure 1.16: 802.11 and OSI Model**

Thus all the components in the 802.11 architecture fall into either the media access control (MAC) sub-layer of the data-link layer or the physical layer.
1.8.5.1 802.11 MAC Frame

The 802.11 MAC frame, as depicted in Fig. 1.17, consists of a MAC header, the frame body, and a frame check sequence (FCS) with corresponding number of bytes for each field. The Duration ID field is 2 bytes long and contains the duration value for each of the fields. For control packets, this field also carries the association identity (AID) of the transmitting station. There are four address fields to accommodate the possibility of message relay. The appearance of address in a field depends on the packet being forwarded through the Distribution System (DS). The contents of address fields in MAC Header (Fig. 1.17) are determined by the values of the ‘To DS’ and ‘From DS’ bits in the Frame Control field (Fig. 1.18).

<table>
<thead>
<tr>
<th>MAC HEADER</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Bytes</td>
</tr>
<tr>
<td>Frame Control</td>
</tr>
</tbody>
</table>

Figure 1.17: 802.11 MAC Frame Format

The Frame Control field contains the control information for defining the type of 802.11 MAC frame and providing information necessary for the following fields to understand how to process the MAC frame. The Frame Control field is 2 bytes long, the bit-wise breakdown of which has been depicted in Fig. 1.18.

<table>
<thead>
<tr>
<th>Protocol Version</th>
<th>Type</th>
<th>Subtype</th>
<th>To DS</th>
<th>From DS</th>
<th>More fragments</th>
<th>Retry</th>
<th>Power Mgt.</th>
<th>More Data</th>
<th>WEP</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Bits</td>
<td>2 Bits</td>
<td>4 Bits</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
</tr>
</tbody>
</table>

Figure 1.18: Contents of the Frame Control field
Here the first two bits are the Protocol Version that indicate the version of 802.11; Type field (2 bits) and Sub Type field (4 bits) combination describes the type of frame and its function; ‘To DS’ and ‘From DS’ fields of one bit each are either set to ‘1’ or ‘0’, indicating whether the packet was sent to or received from the Distribution System (For messages within a single basic service set, both of these fields would be set to 0); More Fragments bit would be set to ‘1’ if there are more fragments of current packet; The Retry bit is set to ‘1’ in case current packet is a retransmission of a previous attempt; Power Management bit is set to ‘1’ if the node will enter power save mode after the current transmission; More Data bit is set to ‘1’ if packets have been buffered and are waiting to be delivered to the destination node; WEP (Wired Equivalent Privacy) bit is set to ‘1’ if the content (payload) of the packet has been encrypted using the WEP algorithm; and Order bit is set to ‘1’ if the packets are strictly ordered, for example in the case of voice over IP.

1.9 SECURITY IN GENERAL

Though modern technology for handling information has made communication quicker, easier and more convenient, it has also brought along security issues. Ever since there has been a need to keep one’s personal possessions safe, especially the property, that requires best possible security. Since the early days of civilization, human beings have always worried for the security whether it is through bridges, moats or walls and are carried forward even at present. The Great Wall of China is one of the greatest examples of ancient security symbols. In modern times, we have alarm systems, telephone lines, CCTVs and even the computers that keep us safe by one or the other way from various threats. Security may be personal — provided by ourselves or provided by government agencies or some other organization. Security of home, appliances, property, vehicles, automated substations, software, bank transactions and many more, prove that we
require security in one form or the other [34-36]. Basically, security refers to the mechanisms and procedures that are designed to ensure that appropriate checks on information access are in place and effective too. In the present era of information, all money transactions, electronic communication applications, power plants, airlines flight schedules/bookings, railways, wind farms, etc., the transmission of messages and password security issues are all managed online through internet where information security is an extremely important concern these days [19, 22, 37-39]. Thus it is rightly said that we all are security consumers in one way or the other. As described earlier, information transfer is a making feature of this era. So security concerns during information retrieval, processing and transfer are the major concern nowadays.

**1.10 NEED OF SECURITY IN WIRELESS NETWORKS**

Wireless communication has become an integral need of the day for almost everyone. Having advantages of providing mobility and flexibility, it finds its application in modern corporate offices, homes, networking, business hot-spots, conference rooms, industrial warehouses, campus, residences, cafe and many other spheres of corporate and personal environment. Wireless in general means without any wire but the term has become a synonym of radio communication. Nowadays wireless communication is extensively used in networking for preparing wireless LANs commonly known as WLAN. With use and growth of internet, the WLAN has become all the more popular. However, from the outset, the Internet was based on open network architecture with computer-based nodes and without network security. Due to these factors it was vulnerable to attackers and hackers. The WLANs have become increasing popular in last decade. The increase in demand is due to large number of added advantages that come with WLAN, namely: suppleness and mobility. With the increase of popularity of wireless networks, the security has become the leading
Introduction

concern. In recent years, it has been witnessed that there is a great inclination towards wireless technology and thus it is getting penetrated in computers and telephone networks that results in the cropping-up of a wide range of networks called wireless networks. On account of various advantages of these networks, there has been an exponential growth in both deployment and implementation of such networks. Since these networks are not limited by any physical boundaries, the information on these networks is usually prone to various forms of attacks. Thus with increase in need of wireless networks, the security aspect of such networks ought to be analyzed. As compared to wired networks where attacks can be limited by restricting the network access of the intruder using physical boundaries such as walls, security doors or barbed wire, these methods do not work in a wireless network as the information is transferred using electromagnetic waves which can pass through any of such physical boundaries, thus getting it much and much tougher task in securing these networks from intruders.

1.11 CRYPTOGRAPHY IN SECURITY ALGORITHMS

Cryptography is one of the most basic techniques implemented in security algorithms for securing the information. Cryptography is basically secure transfer of messages in the presence of an adversary. Since ancient times, for secure transfer of messages, various means have been adopted by human beings so as to ensure that only the sender and the addressee be able to interpret the message, while it should be devoid of significant meaning to a third party. Even today, this practice continues with more fervour. Cryptography is a science of rendering the message unreadable so that the information is not passed to an unintended receiver. Compared to stegnography, which is basically a technique of hiding a message by camouflaging it with other data, cryptography converts the original message, commonly called the plaintext, to some form, such that only the intended receiver can recover the information. From the Jefferson wheel that used
simple cryptography schemes to transmit secret military messages during the
world war II to modern cryptographic algorithms that run in mobile network
nodes, cryptography continues to be a vital area of concern. Today large
amount of data are transferred over wireless, wired, and optical
communication channels. Hence privacy and security of this data is of prime
concern in various application areas of communication. In certain data
transfer applications, this data is highly confidential and sensitive and needs
to be protected against various attacks. Growth of internet users is attributed
mainly to confidentiality and accuracy of information. Wireless networks
transmit in unguarded space and thus are also subject to malicious acts.
Various networks, like Dense Wavelength-Division Multiplexing (DWDM)
optical networks, which can transport a massive cumulative traffic (terabits
per second per single fibre); too have the issues of information privacy and
network security. As a result, numbers of cipher keys have been developed
while cipher-key distribution, identification of malicious actors, source
authentication, physical-link signature identification, countermeasures, and
so forth have been the major area of research efforts from information
security point of view. As the messenger was subject to interception and the
message was subject to the integrity of the messenger, even in modern
cryptography, there is always a threat that the message signal could be
subjected to interception and thus to avoid this various integrity check
algorithms are employed. Since, cryptography suffers from these flaws;
methods are developed by the researchers from time to time in order to
ensure that the message gets received at its destination safe and untampered
[40]. Fig. 1.19 depicts the classic use of cryptography and underlines the
basic terminology used in it.
Here a sender first initiates the plaintext \( P_t \) that gets encrypted by implementing an encryption technology on the basis of certain algorithm. The result is a message which is substantially different from \( P_t \) and is known as *cipher-text* \( C_t \), which is readable only by specific users who know the process to decrypt it. To recover the original text, the receiver uses the inverse encryption process known as *decryption*. Cryptography is mainly classified into two categories i.e, symmetric cryptography and asymmetric cryptography.

### 1.11.1 Symmetric Cryptography

In symmetric cryptography as has been depicted, in Fig. 1.20, the Sender Node (SN) and the Receiver Node (RN) use the same key for encryption and decryption. Although in this case, the mechanism becomes simple but has certain limitations too. Firstly, it is easy for the Attacker Node (AN) to decrypt the message. Secondly number of keys required is very large. Due to these two limitations, generally symmetric key cryptography algorithms are rarely employed to design security algorithms. Fig. 1.20 enumerates the same terminology in modern era for wireless communication.

---

**Figure 1.19: Cryptography terminology**
1.11.2 Asymmetric Cryptography

In Asymmetric cryptography lesser numbers of keys are needed for a given number of users. This type of cryptography makes use of two keys: public key ($K_{pub}$) and private key ($K_{priv}$) for encryption and decryption. The Sender Node (SN) uses public key ($K_{pub}$) for encryption whereas the Receiver Node (RN) makes use of a private key ($K_{priv}$) for decryption. A general idea of asymmetric cryptography is shown in Fig. 1.21.
1.12 ATTACKS ON WLANS

With the increase in deployment of various network and communication devices viz., PSTN networks, wired local area network, wireless LAN and cellular networks shown in Fig. 1.22 have made data and information transfer effortless. However with growth of these networks, attacks against them have become very common. These attacks exasperate the user and the whole idea of using the networks seems to be futile.

![Figure 1.22: Application areas of networks and communication devices](image)

It has been noticed that during the past few years, wireless LAN security threats have enhanced to a great extent that has affected users, vendors as well as the manufacturers. An attacker can interpret vulnerabilities of wireless networks and create different forms of attacks that could be implemented by getting some training and use of appropriate software. According to recent news, the hacker who shook the US intelligence machinery and had world leaders railing against Washington for spying on them, Snowden, spent a week in Delhi, INDIA honing his hacking skills at an institute in the national capital.

"Snowden was a certified ethical hacker and hence he chose a fast-track course. It didn't take him much time to figure out how to create exploit-
attacks and hack wireless networks. He was able to interpret vulnerabilities and outcomes in security testing," said Sisir Pandey, technical manager in information security at Koenig who trained Snowden on a network security tool [41]. This recent incident has again drawn attention to the need of security in wireless networks. The level of attacks has been getting more and more complex, as attack applications are becoming much sophisticated and highly automated. The type of attack, the level of attack and its consequences may vary from network to network. Some of the most common attacks affecting a Wireless LAN are as follows:-

1.12.1 Dictionary attack

A dictionary attack exploits the basic tendency of users to use weak passwords. During the process of this attack, the wireless LAN (WLAN) is subjected to defeat by determining its secret key by repeatedly trying different passwords from a standard set, which in cryptography is known as the dictionary; hence the name Dictionary Attack [42-44]. Let us consider a challenge–response transaction between a Sender Node (SN) and Receiver Node (RN) which is commonly used in authentication protocols. In this transaction, both nodes can generate a random string. This string is transmitted to the other node so that it can encrypt the string in association with its key. The encrypted response is returned to the sender node. This process guarantees that the peer node actually possess the appropriate key. Let us consider a typical situation in which a sender SN generates a random data packet ($D_p$) and sends it to RN after encrypting it using the secret key. This forms a challenge for the Receiver Node (RN). RN decrypts, calculates ($D_{p+1}$) and returns it back to the sender after encryption.

However, if secret key is a weakly chosen password, and it belongs to a set of words called dictionary, usually denoted by D, then there is a great possibility that the transaction in challenge-response process can be attacked. The intruder guesses a key $k_g \in D$ and tries to decrypt both messages $D_p$ and
D_{p+1} with the guessed key k_{g}. Using this key, the intruder obtains two values, P and Q respectively. If P = Q+1, then the attacker gets successful in judging the correct secret key. Although there are certain algorithms which can work against such offline dictionary attacks, among which Secure Remote Password and Encrypted Key Exchange are some of the popular ones and are briefly discussed as under:-

1.12.1.1 Secure Remote Password

Secure Remote Password (SRP) is a protocol of password authentication and key-exchange, suitable for authenticating users, while allowing them to exchange keys over an un-trusted network. SRP resists dictionary attacks being initiated due to the use of weak passwords by the users and are known to have very good secrecy [45].

1.12.1.1.a. SRP Usage

This protocol is based on the concept of communication between user and a server and was suggested by Thomas Wu, where the combination of zero-knowledge proofs with asymmetric key-exchange protocols was developed and thus named as secure remote password (SRP) [45]. Let P be a user and Q be a server. Following steps are performed by P and Q before initiating the SRP protocol:

1. P and Q agree on the underlying finite field.
2. P picks a password (pwd) and a random bit pattern usually called random salt (S_{r}), and computes the verifier v = g K_{priv}, where K_{priv} = #( S_{r}, pwd) is the long-term private key and # is a cryptographic hash function.
3. Q stores the verifier (v) and the corresponding random salt pattern (S_{r}) and now P and Q can engage in the SRP protocol.
This protocol eliminates plaintext equivalence and is a verifier-based protocol. In this protocol, password is private entropy and verifier is a public key. It is quiet easy to compute the verifier from the password, but deriving the password for a given the verifier, is computationally not feasible. However, unlike with a public key, the entity, doing the validation can keep the verifier secret. All SRP computations are carried out on the finite field \((F_n)\), where \(n\) is a large prime number and \(g\) is a generator of \(F_n\).

1.12.1.1.b. SRP Algorithm

This algorithm is based on the data transfer between two communicating entities called user P and user Q. To initiate SRP, first of all, user P sends its username \(P\) to server \(Q\). On receiving it, \(Q\) looks up \(P\)'s verifier \(v\) and salt \(S_r\) and sends \(P\) the salt. This is followed by computation of a long-term private key \(K_{\text{priv}} = \#(S_r, \text{pwd})\) by \(P\) to generate a transient public key \(K_p = g^a\) where \(a\) is randomly chosen from the interval \(1 < a < n\), and sends \(K_p\) to \(Q\). Now \(Q\) computes transient public-key \(K_Q = v + gb\) where \(b\) is randomly chosen from the interval \(1 < a < n\) and sends \(K_Q\) and a random number \(r\) to \(P\).

\(P\) computes \(S = (K_Q - g K_{\text{priv}})^p + r K_{\text{priv}} = gpq + qr K_{\text{priv}}\) and \(Q\) computes \(S = (K_p vr)^q = gpq + qr x\). The values of \(S\) that has been computed by \(P\) and \(Q\) will match if the password \(P\) entered gets match with the value that \(P\) has used in calculating the verifier \(v\) and is stored at \(Q\). At this moment both \(P\) and \(Q\) use a cryptographically strong hash function to compute a session key \(K_{\text{PQ}} = \#(S)\). \(P\) computes \(C_p = \#(K_p, K_Q, K_{\text{PQ}})\) and sends it to \(Q\) as evidence that it has received the session key. \(C_p\) also serves as a challenge. On the other hand \(Q\) computes \(C_p\) itself and matches it with \(P\)'s message. \(Q\) also computes \(C_Q = \#(K_p; C_p; K_{\text{CQ}})\) and this is sent to \(P\) as an evidence to depict that it has also the same session key. Finally \(P\) verifies \(C_Q\), accepts, in case the verification passes, and else abandons it.
1.12.1.2 Encrypted Key Exchange

Encrypted Key Exchange (EKE) is another technique to protect data from off-line dictionary attacks. This scheme is based on a unique combination of an asymmetric key, known as public key and a symmetric key called the secret key. This technique can be used in variety of cryptographic situations. Generally there is tendency of the user to use weak passwords so that they may remember them easily. A dictionary attack exploits this tendency to recover the passwords. However using encrypted key exchange this attack can be nullified to a large extent [46].

1.12.1.2.a. EKE Usage

In EKE protocol, users P and Q serve as the contributing entities in a particular run of the protocol, thereby resulting in a session key which is usually stronger than the shared password and the users can later apply it to encrypt their sensitive data [47]. This algorithm was first suggested by Steven Bellovin and Michael Merritt for the protection of a password protocol against offline dictionary attacks [46].

1.12.1.1.b. EKE Algorithm

The algorithm is based on data transfer between two communicating entities called user P and user Q. To initiate the algorithm, user P forms a public-private key pair (K\text{pub}, K\text{priv}). The next step involves derivation of a secret key (K\text{pwd}) from the given password (pwd) and is followed by encryption of public key (K\text{pub}) by P using (K\text{pwd}) and transfers it to Q. Now Q uses the stored password of P to decrypt the message. In addition Q uses public key (K\text{pub}) with (K\text{pwd}) to encrypt a session key K\text{pq} and sends it back to P. This process is followed by use of this session key K\text{pq} by P to encrypt a unique challenge C\text{p} and sends the encrypted challenge to Q. Now Q decrypts the message to obtain the challenge and generates a unique challenge C\text{q} and then encrypts both C\text{p} and C\text{q} with the session key K\text{pq} and
sends it back to P. This process forms the stage one of the EKE algorithm and is graphically represented in Fig. 1.23.

![EKE Algorithm stage one](image)

**Figure 1.23: EKE Algorithm stage one**

On receiving these, P decrypts this message to obtain $C_P$ and $C_Q$ and compares the former with its own challenge. P matches and verifies the correctness of Q’s response and also encrypts Q’s challenge $C_Q$ with the session key $K_{PQ}$ and sends it back to Q. Now Q decrypts this message and compares it with his own challenge $C_Q$. If they get match, Q knows that P can use $K_{PQ}$ to encrypt subsequent messages.

![EKE Algorithm stage second](image)

**Figure 1.24: EKE Algorithm stage second**
This process forms the stage second of the EKE algorithm as has been represented pictorially in Fig. 1.24.

1.12.1.3 Comparison of SRM and EKE

It has been seen that SRP successfully eliminates plaintext equivalence because neither the server nor the user can access the secret password. This feature clearly distinguishes SRP from EKE and thus SRP is unique in its swapped-secret approach while developing a verifier-based, zero-knowledge protocol that can successfully resist offline dictionary attacks.

1.12.2 Brute Force attack

A Brute Force attack, usually implemented in cryptography, is a comprehensive search of key that can theoretically be employed against any form of encrypted data. This particular attack does the checking of every possible key very systematically till the correct key is deduced. In the worst case, all possible combinations of key are tried thereby exhausting the entire search space and ultimately the key is detected [48]. The key length used in the encryption determines the realistic feasibility of performing a Brute-Force attack. Brute-force attacks can be made less effectual by camouflaging intended sense of the data that is to be encoded. This makes the data unrecognizable to the attacker even if somehow he is able to crack the code and thus renders the hacked data, useless.

1.12.3 DDOS attack

A denial of service occurs when an attacker has engaged most of the resources available with a host on the network, thereby making it unavailable to legitimate users in the network. More specifically, this sort of attack targets the availability of the network, i.e., the network access can be blocked so as to cause larger delays and consumption of network resources such as bandwidth. Such an attack causes denial of some services that are normally offered by a wireless LAN and is known as Denial-of-Service.
(DoS) attack [49]. When a large number of compromised systems attack a particular target, which causes denial of service for all users of the specific targeted system, the attack is called as Distributed Denial-of-Service (DDoS) attack. Thus the targeted system is essentially forced to shut down and therefore the services provided by the system are not offered to the users.

In a typical DDoS attack, a hacker initiates by exploiting vulnerability in one computer system and making it the DDoS master. From this master system, the intruder identifies and communicates with other systems of the network whose security can be compromised. Since the intruder can instruct all controlled machines with a single command, this attack can be a threat to any wireless network.

1.12.4 Wormhole attack

In a wormhole attack, the malicious nodes perturb various routing protocols by creating tunnels [50-51] that affect the decision of choosing the route. Data packets are snooped using these tunnels which may be transmitted in remote location. This creates an illusion of fake routes in the network which appear more efficient. This disturbs the complete routing protocol and may cause undesirable effects in various sections of the network thereby rendering the network weak in terms of security and confidentiality.
Since the wormhole attack is characterized by tunneling, used to capture data packets and depicting the same in some other part of the network, it becomes more dangerous for a wireless network [50-51]. Also as there is no physical boundary limitation in a wireless network, the attacker can create wormholes for any data packet using a wireless link and no physical wire tapping is required.

Let us consider a part of wireless LAN in which node A has a data packet intended for node C through node B as shown in Fig. 1.25. A wormhole attack creates transreceiver in this route so as to modify the
routing path. This situation is shown in Fig. 1.26. As seen from the figure data packet is not available to the node B although the original routing protocol is designed to provide it. Thus similar situations create a different routing protocol which was not pre-assumed and thus makes the network easily vulnerable to threats.

1.12.5 Man-in-the-middle attack and Evil Twin

The other two common attacks namely, the Evil Twin and the Man-in-the-Middle attack are quiet closely related types of attacks where passwords are forged by creating fake users that seem to be genuine. A man-in-the-middle attack refers to an attack in which an attacker intercepts the information between two users by impersonation of legitimate users while the Evil Twin is a malicious server, used to extract sensitive information such as bank details. Evil twin is a term for a malicious Wi-Fi access point that appears to be a legitimate which is provided on the network but in reality has been created by an intruder so as to snoop on wireless communications among Internet surfers. This type of attack may be used by an attacker to steal the passwords of unsuspecting users by either probing the communication link or by phishing.

This type of attack is usually followed by other type of attack and so creates more hazardous effects. Table 1.2 summarizes various attack forms and compares their corresponding modulus operandi.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Various attacks on a wireless LAN</th>
<th>Implementation Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Dictionary attack</td>
<td>Attacker tries different passwords from a set of words in a dictionary</td>
</tr>
<tr>
<td>2.</td>
<td>Brute force attack</td>
<td>Systematically checks all possible keys</td>
</tr>
</tbody>
</table>
1.13 SECURITY ALGORITHMS

The ubiquity of wireless LANs (WLANs) and its deployment in modern offices, schools, universities, work place and even in homes has presented new challenges for network administrators and researchers. With more and more use of these networks, the security is of prime concern and is required in all the places like corporate offices, conference rooms, industrial warehouses, campus, residences, internet cafe etc. Since the information in a wireless LAN is transmitted over electromagnetic waves, it becomes quiet vulnerable to security attacks [47]. Since security of a WLAN is a key issue, a number of standards have been developed from time to time. Firstly in early 80s, a committee IEEE 802 was instrumental in the development of wireless LAN standards and ISM band was developed for token passing MAC protocol. However it was soon realized that this method would lead to the wastage of spectrum. In 1990, a new working group named, IEEE 802.11 was formed by this committee especially dedicated to WLANs. Since then number of standards have been issued by the committee to keep pace with increase in, variety of frequency and bandwidth demands posed by the society [52]. To provide security in a wireless LAN the security algorithms,
namely WEP and WPA may be employed which have been discussed as under:-

1.13.1 Wired Equivalent Privacy (WEP)

The IEEE 802.11 committee had developed Wired Equivalent Privacy (WEP) encryption technique in 1999 which was incorporated in 802.11b standard [52-53]. WEP as the name suggests was developed to introduce security in wireless LAN which is equivalent to that a wired LAN could possess. IEEE 802.11 defined three goals for enhancing security in a WLAN environment [52]:

- Confidentiality: The fundamental goal of WEP is to keep data confidential i.e to keep intruders away from the secret data.

- Access control: The second goal of WEP was to provide an access only to the intended users thereby restricting access to illegitimate users. This feature provides a control on the access to the wireless LAN.

- Data integrity: Although not a primary goal but WEP also aims at checking whether the data which has reached at the sender node is same as it was sent. If the data is altered during transmission, the integrity of the data is lost. WEP includes an added feature which checks its integrity using the CRC-32 algorithm.

These goals were achieved by using specific algorithms in WEP encryption. This algorithm provides two-level security to wireless LAN communication. One is by providing a secret key and other is by using encryption. The secret key comprises of 64 bits with a 24 bit IV (Initialization vector) to provide security. WEP has provisions for a 40 bit and a 104 bit key with fixed size of IV of 24 bits. The key used in WEP is scrambled using a cryptographic function; RC4. RC4 is not particular to WEP but is used frequently in cryptography. The RC4 algorithm is a two
step process consisting of the Key Scheduling Algorithm (KSA) and the Pseudo Random Number Generator (PRGA). WEP concatenates the data and IV with the key stream using the exclusive-or (XOR) function. Another feature particular to WEP is integrity check. An integrity check ensures that packets are not changed during the transmission. This is accomplished using CRC-32 algorithm [52].

WEP is applied to all layer above physical and data link layers for IEEE 802.11b WLANs. This process involves encryption of only the body of data frames, while transmitting the rest of the frame without encryption [54]. A wireless LAN broadcasts the information signals on electromagnetic waves, particularly susceptible to various attacks and eavesdropping [48]. Although WEP was intended to provide security similar to a wired network in a wireless LAN so as to secure it from different types of attacks but ever since it was launched serious flaws have been demonstrated in it [55-56].

1.13.2 Flaws of the WEP

Although increasing the size of the key is known to increase the strength as brute force attack takes longer time to search the key space [48], in case of WEP it has been shown that even on increasing the key size it is not able to resist the attack due to problem of IV (Initialisation Vector) being exhausted. This is because regardless of key size, the insufficient Initialisation Vector space allows an unauthorized person to read the transmitted data using decryption dictionaries [57-58]. Alternatively there are other options too available with the unauthorized users including exploiting the weakness of the RC4 algorithm or exploiting frailty of CRC-32 integrity check [59-60]. The combination of results of Arbaugh, Walker and Borisov et al. demonstrates existence of serious flaws in all of the security mechanisms used by the vast majority of access points supporting the IEEE 802.11 wireless standard [58, 60-61]. Four main flaws in this security algorithm are:-
(i) Initialisation Vector (IV) can be used frequently

Since the IV in WEP is only 24-bit long thus IV space is not perennial and bound to exhaust in a very small time. Typically, a 24-bit IV provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Such a small space of IVs guarantees the reuse of the same keystream. For example, a busy access point, which constantly sends 1500-byte packets at 11 Mbps, will exhaust the space of IVs in 5 hours [60].

(ii) Poor management of key

WEP suffers as far as management of keys is concerned. This standard does not specify how distribution of keys would be accomplished. In most of WEP installations, a single key is used and is distributed among all the users. This may work for a very small organization but is very difficult to manage in a larger one. As a result, all packets in a network are encrypted using a single key. This makes it more luring for an intruder to listen to traffic so as to crack the key and use it. This practice of using same WEP key seriously impacts the security of the system, since a secret that is shared among many users cannot stay very well hidden [60].

(iii) Use of RC-4 algorithm

WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random keystream. Weaknesses in RC4 algorithm are known and it is not strong enough to resist attacks. Fluhrer et al. [58] stated that a weak Initialisation Vector (IV) has about 5% chances of exposing the corresponding key byte. Similarly tests conducted by Stubblefield et al. [62] depicted that 60 to 256 weak IVs were needed to recover a key.
(iv) Use of CRC-32 algorithm

The WEP’s integrity check is based on CRC-32 which is an algorithm used for detecting noise and common errors in transmission. Although CRC-32 is good checksum for detecting errors, but for a cryptographic hash it is not a good choice. Better-designed encryption systems use algorithms such as MD5 or SHA-1 are available but not used in WEP.

However, WEP keeps away a number of attacks using simple approach, due to which this algorithm is still being used as a security measure and hence there is a great scope of exploring it more for practical use.

Due to various problems, the IEEE has recommended both manufacturers and users to move away from WEP and adopt Wi-Fi Protected Access (WPA) which provides a much stronger and currently resilient encryption.

1.13.3 Wi-fi Protected Access (WPA)

Since various flaws of WEP were discovered, the Wi-Fi Alliance came up with Wi-Fi Protected Access (WPA). WPA was discovered as an intermediate solution to various security threats which remained unanswered by WEP, thereby providing the wireless users an immediate solution, until a secure and stable version got created. Although the underlying feature of WPA is also same as that of WEP, it differs in its strength to resist various attacks [63] as it uses a stronger encryption technology. WPA has two variants: AES and TKIP. AES (Advanced Encryption Standards) is a stronger encryption scheme than RC4. TKIP makes use of the RC4 algorithm for encryption and hence is backward compatible with the WEP hardware. Typically Temporal Key Integrity Protocol (TKIP) provides pre-packet key mixing and a message integrity check and utilizes a longer encryption key than WEP which employed a forty-bit key that is relatively
weak. The 128-bit WEP addressed this short-key problem but it has never been a part of an IEEE standard. Each 802.11 vendor implemented 128-bit WEP on its own, and these unique implementations caused problems for heterogeneous environments. By using longer keys and implementation standards, TKIP resolves short-key problem of WEP.

WPA is known to be stronger than WEP as it is effective against many attacks which WEP cannot withstand. It shuts down the network if two packets using the wrong key are sent at any instant of time. Practically when the access point receives these two packets, it assumes the hacker is trying to gain access to the network. Therefore it shuts-off all connections for a moment to avoid the possible compromise of resources on the network. Although it is carried out to provide strength against some wireless attacks, it is used by the attacker to his advantage to bring down the WPA protected wireless LAN. In this situation, a continuous string of unauthorized data could keep the network from operating indefinitely. In this way the security feature is exploited by the attacker to break in to the network.

WPA2 made further changes to WPA by making AES encryption compulsory and uses Counter CBC-MAC Protocol (CCMP) instead of Message Integrity Check (MIC) for integrity check. WPA comes in two modes, enterprise mode and consumer mode. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication while the consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC.

Fig. 1.27 depicts various forms of attacks a wireless LAN can be subjected to and security options available to counter them.
1.14 PROBLEM DEFINITION

Since the world is undergoing an information revolution, today is an era of computer networks, whose popularity is increasing day by day. The additional demand of manoeuvrability in information networks has further been observed in recent years. As a result, the society has witnessed burgeoning of Wireless LANs which have become one of the most popular forms of wireless networks. However, unlike the traditional wired LANs, wireless counterparts are complex in terms of performance and security. Thus with increase in use and deployment of wireless LANs, the need to analyze their performance with optimum security has been very prominent. Since the field of wireless LAN security is comparatively novel, security and performance metrics issues are still concealed and thus they are still required to be explored in much detail. In our research work, firstly we have tried to explore the vulnerability of the wireless LAN standard IEEE 802.11. Later an analysis of two security algorithms namely WEP and WPA for various
numbers of nodes was carried out and various performance parameters were studied. The outline of the piece of research work performed as a part of this thesis is as follows:-

1. Various wireless LAN protocols, their issues in network security and different types of attacks have first been studied in detail.
2. Explored various simulation software being utilized at present by researchers; NS-2 as a specific one was studied and observed as best suited software. Implemented various security algorithms via .tcl and .cc files generated through NS-2.
3. Development of simulation scripts for WEP having various key lengths 64 bit, 128 bit and 256 bit (called WEP-BGS), and their successful implementation through NS-2 to obtain various performance metrics viz. average throughput, average end-to-end delay and average packet delivery fraction, in each case, through Xgraph utility and AWK files generated through NS-2.
4. Varying the size of simulated Wireless LAN, in terms of number of nodes in the network, incorporating WEP-40, WEP-104 and WEP-BGS to obtain a comparative analysis between the three, using different performance metrics. These results help in analyzing effect of increasing the size of a WLAN on different performance metrics when new nodes join it.
5. Simulation of dictionary attack in NS-2 and its application to WEP-40, WEP-104 and also to WEP-BGS. This is followed by carrying out comparisons of time taken to obtain the key when the three different types of WEPs are subjected to these attacks. In addition, the results also help us to compare the effect of dictionary attack on size of the WLAN when implementing these security algorithms.
6. Development of simulation scripts for another security algorithm commonly used in wireless LANs — WPA, its successful implementation through NS-2 and obtaining various performance
metrics viz. average throughput, average end-to-end delay and average packet delivery fraction, through Xgraph utility and AWK files generated with NS-2.

7. Varying the size of simulated Wireless LAN, in terms of number of nodes in the network incorporating WPA and obtaining comparative analysis between the WEP and WPA, using different performance metrics.

1.15 THESIS OUTLINE

Chapter 1 introduces the current internet usage scenario in different parts of the world and focuses on increase in popularity of wireless LANs in recent years. It also introduces the need to secure information networks and discusses types of possible attacks, along with security algorithms which are used nowadays and would be analysed in subsequent chapters.

Chapter 2 provides a digest about the study of literature done as part of the research presented in this thesis. It includes the study of various types of networks, issues related to their security, various security algorithms used and performance metrics which are helpful in analysis of the popular security algorithms.

Chapter 3 deals with simulation details and the NS-2 simulator in particular.

Chapter 4 provides the detail description of WEP and includes the description of its algorithms along simulation results for WEP-40 as well as its two other variants WEP-104 and WEP-BGS.

Chapter 5 details WPA algorithm along with simulations results for the same and brings out various variations and average values for different performance metrics for different number of nodes.
Chapter 6 emphasis results of simulations for the two algorithms with reference to its vulnerability to dictionary attack, throughput and end-to-end delay. It also includes the comparative analysis of the results so obtained.

Chapter 7 concludes this study along with scope of future work.

1.16 CHAPTER COMPENDIUM

This chapter starts with historical evolution of communication systems where different technologies instrumental in development are introduced, ultimately leading to latest development. Since information is an important feature of modern world, information and types of information systems which are used in modelling, maintenance and management of information are discussed in brief. After this, detail is provided on growth of information networks which is reinforced by invent and usage of internet. This detail is supplemented by a number of statistical results using graphs and tables. This leads to the classification of information networks in two broad categories viz; wired and wireless networks. Both types of networks are introduced and compared in terms of various parameters. Then a general view of security and its need in every day routine is emphasized followed by the specific need of security in wireless network is stressed upon. Some basic features and techniques such as cryptography and its types have also been discussed in this chapter. In addition to the various types of attacks which are prevalent on wireless network, the chapter also discusses two popular security algorithms namely the WEP and WPA, in brief. Finally the chapter concludes with the outline of the thesis, describing the contents of rest of the chapters.