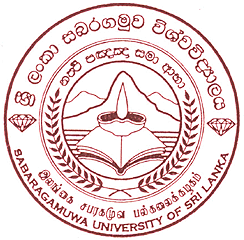
ASSIGNMENT 1



**DATA COMMUNICATION & NETWORKING ISSUES IN REAL WORLD**

J.D.N.M. Jayalath

13/AS/100

EP 1774

Data Communication & Computer Networks

(PST 32227)

Department of Physical Sciences & Technology

**Introduction**

Wireless communications networks incorporate a broad range of technologies, including electrochemical materials, electronic devices and circuits, antennas, digital signal processing algorithms, network control protocols, and cryptography. Although all of these technologies are well advanced in other applications, wireless systems introduce a set of constraints and challenges beyond those addressed in the evolution of other communications networks, such as the (wireline) public switched telephone network and the Internet. These special constraints make it exceedingly difficult to design affordable wireless systems that meet every need. The challenges can be grouped into three categories: mobility, connectivity, and energy.

Mobility is a fundamental feature of untethered communications networks. Portable, wireless communications devices significantly enhance the mobility of users, but they also pose network design difficulties. As the communications devices move, the network has to rearrange itself. To deliver information to a mobile terminal, the network has to learn the new location(s) of the terminal and change the routing of information accordingly, sometimes at very high speeds. The rerouting must be done seamlessly without any perceived interruption of service**.**

A wide variety of problems arise when mobile wireless communications terminals send and receive signals over the air. The signals of all the terminals are subject to mutual interference. The characteristics of the propagation medium change randomly as users move, and the mobile radio channel introduces random variation in the received signal power and other distortions, such as frequency shifts and the spreading of signals over time. Signals that travel over the air are also more vulnerable to jamming and interception than are those transmitted through wires or fibres. These limitations are often addressed with a combination of sophisticated signal processing techniques and antennas. However, these solutions add to the complexity of portable communications devices and increase power requirements.

Wireless systems pose two types of power challenges. First, when power is radiated from an antenna, very little of it typically reaches the receiver, a phenomenon known as path loss. This problem can be partly overcome with increased transmit power, special types of antennas, and other solutions. Second, wireless terminals often carry their own power supplies in the form of batteries. Battery life is limited and is influenced by many aspects of terminal design as well as the technology of the network infrastructure. Scarce power constrains the signal processing capabilities and transmit power of the mobile terminal, motivating efforts to keep these units as simple as possible. However, a low-power design cannot accommodate the most sophisticated techniques available to cope with the vagaries of the wireless channel and support the network protocols of mobility management. In the absence of research breakthroughs that simplify these techniques, the only solution is to increase the complexity of the network, which needs to compensate for the simplicity of portable communications devices.

The challenges related to mobility, connectivity, and energy have stimulated a high level of R&D activity in the telecommunications industry and academia. Still, a chasm remains between the capabilities of wired and wireless communications systems. Even as commercial wireless systems evolve, additional features will be needed to meet military requirements for untethered communications. Military applications introduce additional challenges because the systems need to be rapidly deployable on mobile platforms in any one of a diverse range of operating environments; they need to interoperate with other systems; and they need protection against enemy attempts to jam, intercept, and alter information.

**1) Problems in wireless channel transforming**

The characteristics of the radio channel impose fundamental limits on the range, data rate, and quality of wireless communications. The performance limits are influenced by several factors, most significantly the propagation environment and user mobility pattern. For example, the indoor radio channels typically support higher data rates with better reliability than does the outdoor channel used by persons moving rapidly.

**1.1) Path loss**

Path loss is equal to the received power divided by the transmitted power, and this loss is a function of the transmitter-receiver separation. For a given transmit power, a path loss model3predicts the received power level at some distance from the transmitter. The simplest model for path loss, which captures the key characteristics for most channels, is an exponential relationship: The received signal power is proportional to the transmit power and inversely proportional to the square of the transmission frequency and the transmitter-receiver distance raised to the power of a ''path loss exponent."

**1.2) Shadow fading**

A received signal is often blocked by hills or buildings outdoors and furniture or walls indoors. The received signal power is in fact a random variable that depends on the number and dielectric properties of the obstructing objects. Signal variation due to these obstructions is called shadow fading.

**1.3) Interference**

Users of wireless communications systems can experience interference from various sources. One source is frequency reuse, a popular technique for increasing the number of users in a given region who can be supported by a particular set of frequencies. Cellular systems reuse frequencies at spatially separated locations, taking advantage of the falloff in received signal power with distance. The downside of frequency reuse is the introduction of co-channel interference, which increases the noise floor and degrades performance.

**1.4) Satellite channels**

Satellite channels have inherent advantages over terrestrial radio channels. Multipath fading is rare because a signal propagating skyward does not experience much reflection from surrounding objects. Moreover, most satellite systems operate in the gigahertz frequency range, allowing for large-bandwidth communication links that support very high bit rates.

**2) Capacity Limits of Wireless Channels**

The capacity limits of wireless channels with all the impairments outlined in the previous section is quite challenging. A relatively simple lower bound for a channel capacity that varies over time is the Shannon capacity under the worst-case propagation conditions. This is often a good bound to apply in practice because many communication links are designed to have acceptable performance even under the worst conditions. However, this design wastes resources because typical operating conditions are generally much better than the worst-case scenario. For channels that exhibit shadow fading or multipath fading, the channel capacity under worst-case fading conditions is close to zero. The capacity of these fading channels increases greatly when the data rate, power, and transmission are adapted using sophisticated modulation techniques.

**3) Channel access**

In many modern wireless systems, multiple users share the same bandwidth, creating a need for a protocol that ensures efficient, equitable channel access. Wireless-channel access issues are complicated by the variability and statistical nature of user traffic: Voice traffic typically requires a 40 percent duty cycle (i.e., the channel is used 40 percent of the time), whereas data traffic tends to come in bursts with a much lower duty cycle. All traffic generally varies depending on how many transmitters are active. In addition, many new applications do not exhibit the symmetric two-way flow of voice data that is characteristic of standard telephone service. In typical surfing of the World Wide Web, for example, 100 to 1,000 times more data flows to the user than from the user. This variability and asymmetry are creating a need for new access strategies for digital integrated networks.

**Network Issues**

**1) Architecture**

The choice of an architecture for a two-way wireless network involves numerous issues dealing with the most fundamental aspects of network design. The primary issue is whether to use a peer-to-peer or a base-station-oriented network configuration. In a peer-to-peer architecture, communication flows directly among the nodes in the network and the end-to-end process consists of one or more individual communication links. In a base-station-oriented architecture, communication flows from network nodes to a single central hub.

The choice of a peer-to-peer or base-station-oriented architecture depends on many factors. Peer-to-peer architectures are more reconfigurable and do not necessarily have a single point of failure, enabling a more dynamic topology. The multiple hops in the typical end-to-end link offer the advantage of extended communication range, but if one of the nodes fails then the localized link path needs to be re-established. Base-station-oriented architectures tend to be more reliable because there is only one hop between the network node and central hub. In addition, this design tends to be more cost-efficient because centralized functions at the hub station can control access, routing, and resource allocation. Another problem with peer-to-peer architecture is the significant co-site interference that arises for multiple users in close proximity to each other—a problem that can be averted in a base-station-oriented architecture by the coordinated use of transmission frequencies or time slots.

**2) Physical Resource Allocation**

Any system using a fixed assignment of network resources needs to be designed based on worst-case signal propagation and interference assumptions. A more efficient strategy is dynamic resource allocation, in which channels, data rates, and power levels are assigned depending on the current interference, propagation, and traffic conditions. For cellular systems, dynamic resource allocation includes assignment of channels to base stations. Dynamic channel allocation in cellular systems improves channel efficiency by a factor of two or more, even when using simple algorithms. However, analyses of dynamic resource allocation to date have been based on fairly simplistic system assumptions, such as fixed traffic intensity, homogenous user demands, fixed reuse constraints, and static channels and users. Little work has been done on resource allocation strategies that consider simultaneous, random variations in traffic, propagation, and user mobility. The extent to which system performance can be improved under realistic conditions remains an open and challenging research problem with respect to both cellular and packet-radio architectures. Previous research has focused primarily on cellular systems; little attention has been devoted to peer-to-peer networks.

3) **Wireless Overlay Networks**

No single network technology can simultaneously offer wide-area coverage, high bandwidth, and low latency. In general, networks that span small geographical areas (e.g., LANs) tend to support high bandwidth and low latency, whereas networks that span large geographical areas (e.g., satellite networks) tend to support low bandwidth and high latency. To yield flexible connectivity over wide areas, a wireless internetwork needs to be formed from multiple wide area networks, medium area networks, and local-area networks interconnected by wired or wireless segments. This internetwork is called a wireless overlay network because the WANs are laid on top of the medium- and local-area networks to form a multi layered network hierarchy. A user operating within the LAN enjoys high bandwidth and low latency, but when communicating outside the local coverage area the user accesses a wider-area network within the hierarchy, typically sacrificing some bandwidth or latency in the process.

**4) Resource Discovery**

New protocols are being developed to support convenient operations by mobile users. One example is the service location protocol, which allows user agents to determine access information for generic network services such as printing, faxing, schedule management, file system access, and backup. A directory agent delivers universal resource locators (URLs) to user agents, which use the URLs to access service agents. New service agents can register or withdraw their URLs as needed. Much of the protocol research is geared toward enabling the identification of directory agents in unfamiliar environments. Other strategies based on modifications to directory services have been proposed as well.

**Some other network issues**

**1) Dead drop**

A PC, phone, access point or printer is connected to the wall jack and the connection is not activated. The switch port does not show a link light, nor does the network adapter.

Dead drops are commonly simple problems that occur when a connection is not patched through to the wall jack. In many organizations, only those connections that are actively being used are patched. When offices or meeting rooms are moved around, sometimes the network jacks are not tested for the new users, or drops that are intentionally left disconnected may not be properly documented. Additionally, the switch port may be administratively disabled.

**2) Can’t get an IP address**

The network appears down or inoperable. The operating system may alert that an address was not received from the DHCP server. After checking the network adapter status, no address may be configured.

No address has been received from the DHCP server. The DHCP server may be out of addresses, the server service may be down, the end device may be configured to use a static address instead of a DHCP address, or the DHCP request from the end device never made it to the server in the first place. This may be the case especially if a new device is configured for a VLAN that is not set up to forward DHCP requests to the DHCP server.

**3) Can’t connect to the application server**

The application the user is trying to open may alert that it cannot connect to the application server. This can be the case when using e-mail applications or CRM Applications. The common complaint into the help desk is that the network is down, even though this is not the true problem.

Several things can cause this event. The key question to ask the user is whether this problem happens constantly or only sporadically. If the user has a proper IP address for the connection they are on, there may be a routing issue on the network between the user and server. This can be verified with a simple ping. If connectivity is lost sporadically, this can be caused by a busy server that is not responsive to client requests.

**4) Incorrect VLAN assignment**

When installing new services on the network such as wireless or VoIP, VLANs are typically used to isolate this traffic from other users. This requires each switch port supporting these services to be configured for the proper VLAN. If this is not done properly, the service may not work. The IP Phone may not register with the call manager, the PC connected to the phone may not be able to connect to key servers, or the wireless users may not get proper addressing for the wireless environment.

The switches responsible for connecting these services have not been properly configured. Perhaps it was not communicated within the organization to reconfigure certain ports to support new services.

**5) Duplex mismatch**

With a duplex mismatch, the connection will work, just poorly. The link lights will become active on both the switch and network adapter. Network performance will suffer greatly, with throughput dropping to 100Kbps or lower.

One side of the connection is operating in full duplex (transmit and receive at the same time) and the other device is operating in half duplex (transmit OR receive at one time). The full duplex side does not have to wait to transmit, it is configured to transmit whether it is receiving or not. The half-duplex side must wait until it is not receiving in order to transmit. This means that the full duplex side has the potential to interrupt the half duplex side, causing the half duplex side to abort transmission. If transmission is aborted, the frame will need to be retransmitted. This will dramatically reduce the bandwidth the half duplex side is able to make use of.

**6) Slow application performance**

The application appears sluggish. It may freeze on a certain screen or halt while accessing data. Often, the network is blamed for these issues.

Exonerating the network in application performance problems can assist server maintenance personnel to take out the guesswork and isolate the issue to the right place. Many issues can cause an application to slow down. Among the most common causes are server backups occurring during production hours, slow response from database servers, and packet loss on the network. From a network technician’s point of view, the most important thing to determine is whether the problem is caused by the server or by the network. To determine this, a capture of application traffic can be collected from a client machine. Look for any retransmissions between the client and server. If retransmissions exist, there is packet loss on the network, which severely affects application performance. If there are no retransmissions and connectivity between client and server is established, the problem is likely in the server and can be monitored from that perspective.

**7) Printing problems**

Printing does not consistently work on the network. A printer may appear available, but print jobs that are sent to it are not completed.

Determine if only one user is experiencing this problem or if several people have the same issue. If only one user is having the issue, it may be that the PC is not mapped correctly to the print server. If this is not the cause, the network between client and printer may be to blame. Packet loss can cause printing problems, as well as network connectivity problems on the printer itself.

**8) Poor or bad cable**

If the client PC is able to link to the network, performance may be poor. The PC may not be able to connect at all.

In networks today, Gigabit to the desktop is common. Gigabit requires four pairs of cable, so anything lower than Category 5 will not work for Gig. In older buildings this must be taken into consideration. In addition, any amount of untwisting of the cable (often near the RJ-45 termination or patch panel) can cause signal loss. This will result in FCS Errors on the switch ports or network adapters.

**9) DNS problems**

The user cannot access the internet or key applications. The network appears to be down.

Domain Name Services may be to blame. The client PC cannot resolve the name of the server with the IP address of that server, so it will not send a connection request. This is often caused by having the wrong DNS server configured on the client, sending DNS requests that the server does not have in its database, or packet loss on the network. DNS is a UDP-based protocol, so packets that are lost will not be retransmitted, causing DNS to fail.

**10) Wireless client can’t connect**

The client can detect the wireless access point, but it cannot connect to the wireless network.

Security credentials, wireless channel interference, and dead spots can cause this problem. Since wireless is invisible, it can be very difficult to track these problems down without a proper wireless tool.

**End-to-End System Design Issues**

Most end-to-end system design issues, such as security, design tools, and interoperability with other systems, are relevant to any wireless application. However, some end-to-end design issues depend on the application to be supported by the network. For example, videoconferencing is an extremely challenging application for a wireless system because of its high bandwidth requirement and strict constraints on delayed end-to-end transmissions. To support this application, the capability to adapt to channel conditions, perhaps through a slight degradation in image quality, might be built into the end-to-end system protocols. Similarly, many military command-and-control operations require the capability to assign priorities to certain messages, and this flexibility needs to be built into the system. The following sections deal with three key end-to-end design issues for wireless systems: application-level adaptations, quality of service, and system security.

**1) Application-Level Adaptation**

A system can adapt to the variability in mobile client applications in three ways. One approach is to exploit data-type-specific lose compression mechanisms and use data semantics to determine how information can be compressed and prioritized and route to the client. A second approach is on-the-fly adaptation involving the transcoding of data into a representation that can be handled by the end application. The third approach is to push the complexity away from the mobile clients and servers into proxies, which are often used in wired networks but are not currently optimized for wireless applications.

Introduced in response to security concerns, the proxy approach is a new paradigm for distributed applications. A proxy is an intermediary that resides between the client and server—outside the client's security firewall—to filter network packets on behalf of the client. Proxies provide a convenient place to change data representations and route to the client, perform type-specific compressions, cache data for rapid re-access, and fetch data in anticipation of access. By supporting the adaptation to network variations in bandwidth, latency, and link error rates as well as to hardware and software variations, proxies enable client applications running on limited-capability end nodes to appear as if they were running on high-end, well-connected machines. Low-end clients (e.g., PDAs) have limited processing capabilities due to small displays and memory, relatively slow processors, and limited-capability software and run-time environments.

**2) Quality of Service**

Quality of service refers to traffic-dependent performance metrics—bandwidth, end-to-end latency, or likelihood of message loss—that a connection must have or can tolerate for the type of data transmitted. A network's admission-control mechanisms, which are invoked whenever a new connection is initiated, provide assurance that Quality of service requirements will be met; a new connection is aborted if its Quality of service requirements cannot be met. Attention to Quality of service issues is increasing because of at least two converging trends: the growing market for applications (e.g., video) that require real-time service, and the evident interest in using the Internet for a range of activities that are critical to both the public and private sectors.

Wireless communications introduce additional Quality of service issues. The Quality of service guarantees for expected loss rates, latencies, and bandwidths were developed based on the assumption that switched, fibre-optic wired networks would be used. Such networks feature low link-error rates, easily predicted link bandwidths, and Quality of service parameters that are largely determined by how the queues are managed within the switches. As a result, losses are due almost entirely congestion-related queue overflows. Wireless links, on the other hand, have high bit-error rates, high latencies due to link layer retransmissions, and unpredictable link bandwidths. Furthermore, the quality of a wireless link varies over time, and connections can be lost completely. Two wireless end nodes sharing the same link can experience vastly different link bandwidths depending on their relative proximity to the base station, location in a radio fade, or loss of receiver synchronization in a multipath environment. Link quality can also be degraded by interference from a nearby transmitter. In addition, hidden terminals cause time-consuming back-off (i.e., waiting before resending) that further degrades network performance.

**3) Security**

Wireless communication systems are inherently less private than are wired systems because the radio link can be intercepted without any physical tap, undetected by the transmitter and receiver. Wireless networks are therefore especially vulnerable to eavesdropping, usage fraud, and activity monitoring, threats that will grow as wireless banking and other commercial services become available. In addition, both wired and wireless networks need to be designed to maintain the integrity of data and systems and assure the appropriate availability of services. Thus security is an important issue for both commercial and military applications. For purposes of this discussion, which considers key aspects of the information security challenge but is not comprehensive, the issues can be divided into three categories: network security, radio link security, and hardware security.

Network security encompasses end-to-end encryption and measures to prevent fraudulent network access and monitoring. One user-oriented framework distinguishes several levels of end-to-end encryption. Level 0 has no encryption, meaning that anyone with a scanner and knowledge of the communication link design can intercept a transmission. Analog cellular telephones offer this level of security, which has been a problem and has motivated security upgrades in the digital cellular standards. Level 1 provides low-level security such that individual conversations might take a year or more to decrypt. This level is probably secure enough for commercial telephony applications, provided that an equivalent effort would be needed to decrypt subsequent conversations (''perfect forward secrecy"). Level 2 provides increased (perhaps by a factor of 10) security for sensitive information related to electronic commerce, mergers and acquisitions, and contract negotiations. Level 3 provides the most stringent level of security, meeting government and military communications requirements as defined by the appropriate agencies.

Hardware security also has different implications for commercial and military applications, although encryption keys typically need to be protected in both contexts. Commercial systems require sufficient security to prevent the fraudulent use of information in the event of theft or loss, and user databases need to be secured against unauthorized access. The military has similar requirements but at a much higher security level. It also has additional requirements: Military devices need to be protected so that opening them will not reveal any of the specialized hardware or software technology.

**3.1) Technology weaknesses**

Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, Network equipment weaknesses and weaknesses in configuration and security policy.

**3.2) Configuration weaknesses**

Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

**3.3) Security policy weaknesses**

Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy.

**Hardware issues**

Among the hardware issues that are critical to third-generation wireless systems, radio stands out as being central to the military mission. The radio receiver consists of an antenna, RF amplifier, mixer, filters, demodulator, and decoder. Radio signals are received by the antenna, amplified, passed through the mixer and filters, demodulated, and decoded. Transmitters have similar architectures but the operations are performed in reverse order: The data are encoded, modulated, passed through the filters and mixer, amplified, and transmitted through the antenna.

**1) Antennas**

An antenna serves as the interface, or transducer, between the electronic circuitry of a transmitter or receiver and the medium through which radio waves travel. Classical antenna designs include simple stub antennas such as those found on cellular telephones, as well as massive, parallel panels that are aligned in phase to provide flexible electronic steering. While in transit between the transmitter and receiver, the RF signals are subject to a variety of distortions. In addition, they create interference for other communications and provide opportunities for interception. To limit interception and interference and also to conserve power, antennas can be designed so that the RF energy radiates in only a particular direction, providing gain along the intended direction and attenuation in undesired directions.

**2) Other Radio Components**

The evolution of digital technology is transforming radios. Other than antennas, all the components of the radio system—RF amplifier, mixer, filter, demodulator, and decoder—are amenable to either analogue or digital implementation. Many commercial radios and other communications products already use programmable digital modules. There are many advantages to replacing analogue hardware with programmable digital technology, although trade-offs are involved. As noted above, digital technology offers inherent security advantages.

**2.1) Analog-to-Digital Converters (A/D Converters)**

The key enabling component, and the most complex and misunderstood element of wideband software radios, is the A/D converter. Most A/D converters are characterized by maximum clock rate and number of output bits, digital metrics similar to those used to characterize microprocessors or memory devices. However, because signal quality is key, A/D converters are better characterized using analogue characteristics, signal range free from spurious noise, and usable bandwidth. The use of these metrics helps ensure that the critical A/D transition can be accomplished with minimum degradation in signal quality.

**2.2) Filters**

Filters influence not only a radio's signal-processing speed but also its sensitivity, dynamic range, and capability to avert co-site interference. Their importance is reflected in their physical presence: Filters constitute 25 percent of the volume of a typical software radio, in part because several different filters are needed. Improvements in frequency-tuning range and selectivity as well as miniaturization would be helpful, especially for application in handheld devices. The commercial sector continues to rely on older technology whereas the military has unique needs to reduce co-site interference, both within software radios and across multisystem platforms, and cover wide frequency ranges. Existing radios that span wide frequency ranges require combined filters made of new materials that have remarkably flexible and adaptive electrical properties, far beyond older static inductors and capacitors. The new materials and modern filter fabrication techniques will lead to new and smaller implementations of wideband filtering based on the fundamentals of transmission-line techniques. Thus, filters may merit a significant military.

**2.3) Radio Frequency Amplifiers**

The commercial sector is designing ultra linear amplifiers that will process many signals from multiple transmitters and add them coherently to achieve good fidelity. These designs will improve power efficiency and consume less space than traditional amplifiers. However, the commercial sector is unlikely to produce multiband amplifiers, which will be very expensive, anytime soon.

**3)** **Portable Terminal Design**

The small size and portability of wireless communicators provide obvious benefits for users but also introduce challenges for system designers because they limit display, processing, power, and storage capabilities. The following subsections review the limitations and the new technologies designed to overcome them. The commercial sector is making rapid advances in all these areas that the DOD can exploit to good advantage.

**3.1)** **Displays, User Interfaces, and Input Devices**

Small, highly portable devices contain relatively low quality displays. There are three reasons for this. First, portable devices have limited physical space and power available for the display. Second, display pixels cannot be smaller than the resolving limit of the human eye, meaning that the number of pixels in a given display (i.e., the resolution) is limited. In addition, bright colours can be produced only if there is sufficient power for backlights and display elements; otherwise the display is dim and monochrome. For these reasons the user interface of a portable device needs to be designed for monochrome presentations in a very small screen area—a significant impediment to the display of video or high-quality images.

**3.2) Processors**

The successful development of low-power devices with long battery life has placed limits on the raw performance of embedded processors because processing speed and clock cycle directly influence power consumption. New metrics are therefore required to measure the performance of processors for portable applications: millions of instructions per second (MIPS) per watt, a measure of the impact on battery life and heat dissipation in highly integrated systems; MIPS per square millimetre, a measure of the silicon manufacturing costs of the processor; and bytes per task, a measure of the amount of memory that devices need to incorporate to perform signal-processing functions. Because consumers are demanding highly integrated yet portable computing devices, the commercial sector is performing R&D with the aim of increasing processor capabilities while also reducing power requirements.

**3.3) Batteries**

The commercial sector has made tremendous strides in battery technology in recent years because it plays a role in many technologies, ranging from surgical implants to electric cars. Nickel cadmium batteries are the most widely used rechargeable batteries, found in many consumer electronic devices. Most laptop computers now use nickel metal hydride batteries, which have slightly better energy storage per weight and substantially improved energy storage per volume. Lithium ion (Li-Ion) batteries are used in some new portable products, such as small cellular telephones. The energy-storage capacity of Li-Ion batteries is more than twice that of Nickel cadmium technology by both weight and volume. Lithium polymer (Li-Poly) batteries are about 10 percent more efficient than are Li-Ion batteries. Both Li-Ion and Li-Poly batteries use solid electrolytes, making it possible to form the battery into arbitrary shapes, a significant improvement over other battery technologies.

**3.4) Storage**

The disk-drive capacity of information processing devices continues to increase while physical size shrinks, but the 2.5-inch disk widely used in notebook and laptop computers is still too large for handheld devices. In PDAs the disk is replaced by RAM in the form of battery-backed-up static RAM and flash RAM on personal computer multiple component interface access cards, which can cost 30 times more than disk storage per megabyte. Commercial R&D in this area is producing steady, impressive advances that are likely to meet military needs.

**The Internet Related Issues**

**1)** **Loose content controls**

Since there is no censorship over information on the Internet, undesirable and offensive materials may be found on the network. One can obtain pornographic articles, nude pictures and information on hacking, making bombs, manufacturing drugs or committing suicide from the system. There are also concerns that the Internet would be abused by people who use it to spread rumours or false information to cause alarm to the public. As the Internet is a global network, control over materials released outside may be difficult. Content controls on local publications are at present found in the Control of Obscene and Indecent Articles Ordinance. The ordinance has to be reviewed in the light of the free flow of electronic and digital information to the public over the network. There is of course a need to strike a balance between control and free access to information**.**

**2)** **Copyright infringement**

Copying and reproducing data available on-line, on CD-ROM or in other electronic forms including the Internet is much easier than copying from books. This has created problems for copyright enforcement. The difficulty is compounded on the Internet since it is a global network containing vast amount of articles from many sources. The Copyright Ordinance should be examined to see if it has adequate provisions to tackle the problem with copyright infringement on electronic works. Co-operation among governments and international bodies on copyright is needed to come up with an enforceable standard on the global electronic network.

**3) Data security**

Communication on the Internet very often spans across different countries.

In such cases, data are transmitted over communications lines and routed from one network to another before they reach their destinations. Security of personal or private commercial data transmitted over the network is therefore a matter of concern.

Some degree of protection is found in the Telecommunication Ordinance.

Thorough considerations of further safeguards are desirable and should be included in the review of the Telecommunication Ordinance which is being made. The Personal Data (Privacy) Bill should also be scrutinised to see whether it covers providers as any other companies in the way they collect, hold or use the personal data they have such as clients’ account name and billing details. The definition of 'data’ in the Bill does not seem to cover electronic data being transmitted over telecommunications networks and should be studied in detail.

The public should be adequately educated of the implications of transmitting data electronically. Encryption techniques should be introduced to users for their protection. Consideration could also be given to see if there should be a code of practice for providers of telecommunications service to ensure data security and privacy.

**4) Consumer protection**

An increasing number of small businesses and individuals connect to the

Internet indirectly through Internet access service providers. The reliability of the service is of utmost importance especially to those whose businesses make use of the network heavily.

There is at present no regulation over the quality of service of these providers. In applying for the licence, a prospective service provider is required to provide proof of a registered company and to supply information on its directors and principal business. There are concerns that subscribers of such service will suffer if the computer systems of these providers break down or these providers close down their business suddenly. The Government, and perhaps the Consumer Council also, should have a role to play in the education and protection of the consumers.

**References**

[1] Importance of Network Security, found at

http://www.content4reprint.com/computers/security/importance-of-networksecurity-

system.htm

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla(1990). The Architecture of

a Network Level Intrusion Detection System. Technical Report Dept. of

Computer Science, University of New Mexico, New Mexico, August.

[3] A beginner’s guide to network security, CISCO Systems, 2001.

[4] Dieter Gollmann (1999). Computer Security. Wiley.

*Network Security-The Biggest Challenge in Communication* 803

[5] Simmonds, A; Sandilands, P; van Ekert, L (2004).Ontology for Network

Security Attacks. Lecture Notes in Computer Science. Lecture Notes in

Computer Science 3285, pp.317–323.

[6] Michael E. Whitman and Herbert J Mattord(2005).Principle of Information

Security.2nd edition. Thomson Course Technology.

[7] Shailja Pandey (2011).MODERN NETWORK SECURITY: ISSUES AND

CHALLENGES.IJEST, Vol. 3. , pp.4351-4356.