Surviving The Cyber Age

Chapter 4 - Communications

Table of Contents

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Basics of Communications

Communication in the physical sense is about the transmission and reception of waveforms through media. A multitude of different media may be available, and waveforms consist of sequences of values over time and across the spectrum across the media. There's a very wide range of frequencies and amplitudes that can be continuously emitted and received, subject to noise in the channel, and of course the generation and reception may or may not match or be able to withstand variations in the transmission media, including random, natural, and artificial interferences.

Communications in the informational sense is about a transmitter using a scheme of some sort to convey content and a recipient being able to be informed in some way by its receipt. The content part is complicated in that there are two parts to it; the syntactic part and the semantic part.

- The syntactic part was expressed in 1948 by Claude Shannon[1] [2] by expressing communications in terms of uncertainty. The difference between the uncertainty of the recipient before and after reception is, by definition, the information transmitted. This is foundational to much of information theory since then.[3]
- The semantic part is about meaning, and a widely adopted theory of meaning has yet to be developed. However, as a surrogate for meaning in cybernetic systems, we can consider actions taken by the cybernetic system and their effect on the world as reflected in received sensor measurements through the media between actuator and sensor in the context of the control mechanism and its manner of transforming sensory data and context into acts as the meaning of the system. As an example, the meaning of sensed data to a temperature control system is it's effect on subsequent acts to change the current through a heating element, and the meaning of changing the current through the heating element is to change the sensed temperature over time.

Typically communication involves coding of one form or another to match up transmission and reception. In addition, a variety of information theoretic techniques tend to be used including encryption and compression.[4] But even beyond that, there are many techniques such as code book or memes, or the creation of custom languages that adapt over time to match internal structures, such as the networks built up by artificial and natural intelligence that produce and interpret codes, perhaps not in reversible or perfect form of communication, but still transmitting a noisy form of meaning, whatever that is.

A multitude of these may be in place, and it's obvious enough that by tricks like shifting or combining frequencies, amplitudes, coding schemes, media can be used to produce an arbitrarily complex messaging approach. This can drive up the complexity of cohesive interception or interference to at least exceed exponential complexity in the number of media, signaling techniques, coding methodologies, and waveform approaches.

1 Shannon, Claude Elwood (July 1948). "A Mathematical Theory of Communication" (PDF). Bell System Technical Journal. 27 (3): 379–423. doi:10.1002/j.1538-7305.1948.tb01338.x. hdl:11858/00-001M-0000-002C-4314-2.
2 https://en.wikipedia.org/wiki/A_Mathematical_Theory_of_Communication for a discussion.
3 https://en.wikipedia.org/wiki/Information_theory for some more on this topic
4 C. Shannon, 1949, "Communication Theory of Secrecy Systems", which was originally classified (in 1946) and thus actually predated his information theory. Available online at https://all.net/refs/shannon1949.pdf

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Communications architecture

The communications architecture of a cybernetic system uses structures that imply part of its cognitive capabilities and limitations. Those structures are usually composed of combinations of the different communications architectures of groups, entities, and societies and the limits and capabilities of the cybernetic mechanisms of the architectural elements of the mesh, hierarchy, star, and matrix arrangements of components into composites. It is common for the communications structure of the cybernetic system to mirror that of the organization operating it, but this only goes so far, because the technical need to have the cybernetic system meet its operational purposes will cause the organization to fail if its cybernetic capabilities fail.

- **The star** focuses all of the sensors communicating to a single central analytical capability. The central analysis can only process what it gets and can store, and depending on the available bandwidth and storage, it is constrained. For small control systems, this works well enough, but as systems scale, central control introduces a number of problems. These typically include performance, reliability, and scalability.
  - **Performance** is limited by the ability of the center of the star. It has to be able to handle the combined bandwidth of all of the sensors and actuators running at maximum capacity or lose sensory data or control capacity.
  - **Reliability** is limited by the fact that the center of the star is a single point of failure.
  - **Scalability** is limited by the capacity of the center. As long as it can handle additional communications and perform its other functions, it can scale. But it can also be overwhelmed if it is not up to the capacity of the combined bandwidth.
- **The hierarchy** can be thought of as a star where each endpoint is itself a star, and so forth. Hierarchies are more effective in many ways as systems scale, and are the focus of the "watchmaker's dilemma", (A.K.A. the parable of the two watchmakers) used by Nobel laureate Herbert Simon in his 1962 paper, "The Architecture of Complexity". [5]
  - Hierarchies are widely used in organizations with a top decision-maker managing, typically, up to 10 subordinates, each of which does the same, and so forth down the hierarchy. As organizations (or other cybernetic systems) increase in the number of endpoints (also commonly discussed as leaves in a tree structure) more levels of hierarchy are required, but this can be extended without practical limit.
  - Information is compressed on its way up for higher level decisions and structural controls, while lower levels of the hierarchy pay more attention to the specifics and report relevant information up the hierarchy. Higher levels seek to control the information they get and the acts they assert, thus limiting top-level bandwidth and span of communications. Broadcasts are sometimes used (from higher to lower levels), but every level must compress or select what goes up to avoid flooding at the top.
  - The top levels can typically drill down into the details as and if desired, and thus we have the same sort of focus of attention process for human as for other cybernetic

5 http://links.jstor.org/sici?sici=0003-049X%2819621212%29106%3A6%3C467%3ATAOC%3E2.0.CO%3B2-1 "The Architecture of Complexity", Herbert A. Simon, Proceedings of the American Philosophical Society, Vol. 106, No. 6. (Dec. 12, 1962), pp. 467-482.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

systems. Available bandwidth limits the number of simultaneous drill-downs, and because the higher levels control what is sent to them, they see what they want to see and hear what they want to hear.

- **The matrix** is comprised of rows and columns (or a higher number of dimensions) providing connections for transmission in multiple dimensions, increasing effective bandwidth between many pairs of components and particularly useful for efficient execution of specific classes of methods.
  - It has the advantage of providing multiple channels and presumably higher bandwidth to observe sensor data and compress it for different perspectives, but the disadvantage of multiple control signals being sent to actuators and different foci of attention being demanded of sensors. This can then stress sensors and actuators unless properly limited and coordinated to prevent inconsistent or incompatible endpoint configurations and actions.
  - Endpoint resources also grow with the number of dimensions, each one demanding another communications channel for each endpoint. These resources may provide redundancy for communications, if allowed by the mechanisms, and can continue to operate when some dimensions are not operable or able to communicate, but that may also mean that some of the multiple requirements are not being met.
  - Focus of attention is now under the control of multiple masters, and the resources required tend to increase, sometimes to the breaking point. Humans operating in matrix environments tend to suffer from the different contexts they serve, but humans are not as good at handling context changes as computers.
- **The mesh** is a more general sort of network connecting arbitrary pairs of components to fit the happenstance of available resources (like in the Internet) or specifically architected to support specific communications between components to address specific analytical methods efficiently.
  - **Resilience:** The multiple paths produce resilience under low load, but in most cases, mesh architectures are not designed for the specific implementation, and as such, they tend to have different communications limitations along different paths.
  - **Brittleness:** Because they share linkages through intermediate mechanisms, unless designed for all linkages to handle maximum bandwidth requirements, failures or excessive loads will cause delays or lost content. In realtime control situations, this can cause unlimited growth of waves in the physical systems, producing failures of different sorts that are often safety hazards. As the physical world goes, so does the communications environment, and real-world events tend to cause increased load, which causes rapid systemic collapse under some conditions. Similarly, the protocols required to control these complex networks tend to be imperfect and exploitable to conceal some otherwise observable events and confound and confuse the observation and analysis of sensor information through unpredictable delays.
  - **Scalability**: When focus of attention increases with respect to some elements of the mesh, it tends to also increase bandwidth requirements. While mesh networks often provide for more foci of attention because of the resiliency of communications,

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

the architecture also leads to denial of services by overwhelming nodes with flows. This becomes more problematic as the mesh scales and routing becomes more complex. At the same time, because the mesh can be decentralized in terms of control, it can often scale well beyond the level of even hierarchies with better combined decision-making for the overall cybernetic system.

- **Composites** of these structures are often used depending on available resources and structural design matching performance criteria to system requirements. And they also happen through change and history as composites are built from components that happen to use specific architectural components.

Most large scale cybernetic systems are composites because they are 'evolved' over time. With the advancement of technology in the Internet era, distributed control achieved through mesh architectures is increasingly feasible and can be far more resilient than the other approaches at large scale.

In the governance arena, this starts to sound like it's a political statement supporting distributed democratic institutions or anarchy over hierarchy and central control of governments. And of course, the analogy to the star architecture for dictators and autocrats , the hierarchy for big business, and small businesses being more like the mesh is fascinating. But in this context the discussion is not about governance in the political sense. It's about technical structural governance effects on the effectiveness and limitations of communications mechanisms. While the principles are the same, technical communications and control mechanisms do not always accurately reflect the adaptations made by people and the other forces at play in societies, governments, companies, families, and other social structures.

Communications components

The technical components used in communications have specific properties that make them more or less amenable for use in different situations:

- **Actuators and sensors** are used to transmit and receive signals **through media** in order to communicate. Essentially, any actuator identified in actuators that can effect a media, and where a sensor that can detect the effect on the media is present, these actuator, media, and sensor sets can be used to communicate. Rather than try for a comprehensive list, a few examples will help to clarify.
  - In using a toilet, the user (actuator) acts to put bodily fluids (the media) into the toilet. The city wastewater system takes samples and examines it (sensors) for the presence of disease indicators.[6] Thus the user is communicating the presence of communicable disease to the health department.
    - This is a low bandwidth communications system in the sense that the level of disease is only communicated as often as the measurements are analyzed. It is statistically reliable in that once the percentage of diseased users reaches some level, there is a high probability of a communicating the result. It has precision dictated by the statistics based on the number of samples and other factors, and accuracy based on the statistical validity of the measurement methodology.

6 https://www.cdc.gov/nwss/about-data.html provides information on the US national system.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

- In smiling and talking at different points in an interaction, hotel workers are sometimes taught to follow the 10 5 rule[7].
  - At 10 feet from the guest, the worker (actuator) should smile (transmit optically through the space between), and if the guest eye(s) (sensor) sees it, the communication has taken place.
  - At 5 feet from the guest, the worker (actuator) should sincerely greet the guest (verbally transmitting sound through the air as the media), and if the gust hears it (ear as sensor) the communication has taken place.
  - The communication taking place in this and hundreds of other similar transmissions in a day at a hospitality site are intended to convey messages of welcome and support to keep the guest happy and have them remember a positive experience. The messages individually are different ways of coding the overall messaging.
- Online meetings are widely used for business and personal interactions. The scenario usually goes like this:
  - Humans actuate sounds and movements transmitted by optical and sonic signals through the space and air between the user and computer.
  - The computer sensors transform the analog signals into digital sequences and communicate the information to components in the computer that communicate internally transmitting and receiving wave forms over metal indicating 1s and 0s.
  - The endpoint computer ultimately transforms the original waveforms into packets for communications over the Internet.
  - Wires, optical fibers, or wireless media are used to transmit and receive signals representing those packets using optical (light), electrical or electromagnetic (radio) actuators and sensors to communicate from device to device en route to the other participants in the meeting; each device is also a computer and doing internal communications through media to send the packets along their way.
  - The computer of another user receives these signals from the device on the Internet it communicates with using whatever media it connects with, performs similar internal machinations and communications, and transmits the results as signals to speaker and visual display systems. The speaker system transforms digital signals into analog movements that transmit waveforms in the air to users' ear(s) while the display transforms digital signals into analog optical signals transmitted through space to the users' eye(s) where they are received.
  - Experience tells us that there are various properties of the complex systems that limit the ability to communicate, like the number of participants vs the available bandwidth limiting how many videos of what resolution can be seen simultaneously, the quality of sound and images, delays, drop outs, etc.

The list goes on and on, and by now, you should have a good idea of the range of things that can be involved. Any actuator, compatible media, and capable sensor → communication.

7 https://coylehospitality.com/hotels-resorts-inns/what-is-the-10-and-5-staff-rule/

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Symbol Sets and Coding

Symbol sets and coding are the representations used for communication. This subject is covered in substantial depth in “Digital Forensic Evidence Examination” as referenced earlier and available online.[8] As a general introduction, the following supporting information is extracted from testimony given in legal matters over the last several decades.

There are many encoding schemes, and they are used for different purposes. For example, there are many different ways of encoding signals so that they can be received and understood in the presence of noise in communications channels. AM radio uses amplitude modulation in which the amplitude of the waveform varies with the signal. FM radio uses frequency modulation to encode signals (waveforms) by changing the frequency with changes in the waveform. The reason FM typically sounds better and is less noisy is that it is independent of the amplitude of the waveform and thus less susceptible to the most common sorts of noise and distortion in the radio frequency environment.

Digital computers store and process information using representations of various sorts. While the underlying mechanisms have continuous properties, by design, the internal representations of all information in digital computers is in terms of two “atomic” values. These are sometimes referred to as “true” and “false”, “1” and “0”, “on” and “off” (switches), “high” and “low” (voltages), or in other similar pairings. The specific language used tends to vary with the field of use, but they are all used to indicate the binary (two-valued) nature of digital computers. There are no “shades of gray” at this level of representation. I will sometimes call each of these atomic values a “bit”. A bit can be, for example, “1” or “0”, “on” or “off”, and so forth.

In order to work with information more complex than two-valued decisions, such as; characters, digits, words, integers, sentences, formulas, paragraphs, instructions, documents, graphical images, movies, and programs; sequences of bits are used. Because the representation of different sorts of information for different uses is more or less efficient and usable (e.g., the bit sequences used to represent characters in a sentence may not be as easy to use in representing frames in movies), the same bit sequences represent different information in different contexts.

The different ways of representing information as bit sequences is commonly called “coding”. For example, the “code” for the character “A” (upper case A) is different in IBM mainframe computers (using the EBCDIC[9] coding the bit sequence 11010001 represents “A”) than it is in Unix and DOS computers (using the ASCII[10] standard the bit sequence “A” is 01000001), than in Windows™ computers (using the unicode[11] coding scheme, each character is represented by 16 bits, and “A” is 000000000100001), than in “sixbit” (used to save space in some computers where “a” is 100001), than in “ROT13” (where “A” is 01001110), than in BASE64, 7-bit ascii, UTF-8[12], and so forth. The representation of the graphical depiction of “A” seen on the screen is different from the arrangement of dots shown on printed pages, and the codes used to send the character “A” between the computer and printer or display.

8 https://all.net/books/2013-DFE-Examination.pdf
9 Extended Binary Coded Decimal Interchange Code
10 American Standard Code for Information Interchange
11 For details visit http://unicode.org/
12 RFC 2279 - for details visit https://www.ietf.org/rfc/rfc2279.txt – saved as rfc2279.txt

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Computers input key presses and releases as a series of codes that the operating system then encodes into keystrokes in (typically) ASCII, or in the case of Windows™ unicode, coding for storage and retrieval, while the Internet typically encodes messages into Internet Protocol (IP) datagrams for communications between systems. Disk drives use different coding than CD-ROMs, and storage media and transmission media often use codes called checksums to detect accidental alterations in storage or communications.

This use of the term “coding”, “code”, “codes”, and so forth is different in the representation of information as described here from the use of these terms in cryptography (where secret keys may be used to “encrypt” and “decrypt” content, sometimes also called encoding and decoding), in computer programming (also called coding, but also using encoding and decoding to describe changing representations), in data entry (sometimes called “coding” of data), and in other areas. I will try to be clear which type of coding I use when discussing these issues.

Transmission of content and protocols for such

The concept of transmission has been around for a very long time. Any manner in which something is conveyed from one party to another over time or space constitutes transmission.[13] Transmission of information in the form of records and various sorts of copies of records normally involves the coding of content into the format of the sort of record and transmitting the result to the recipient(s). In the digital era, copying of bit sequences is used to produce an external record, often in a different manifestation than the original it copies, and the transmission is typically via transient waveforms such as through signals in wires, changes in voltage values in electronic components, or light transmissiveness in optical media. Protocols (defined and/or agreed methods for systematic exchange of information) are used to implement the methods of communications used to transmit content. While the protocol for transmission in a physical archive might involve the production of physical (e.g., paper) records of the fonds (documents that share the same origin) and including seals, signatures, and/or initials with dates and times for the activities carried out; the transmission protocol in computers can range from the timing mechanisms controlling access to common media (e.g., connection of components to a “bus” with an address and data value doing a “load” of data values on the bus to a memory device based on the bus address) to protocols used for sending sequences of bits on a serial media, to the use of complex embedded protocol systems for global communications like the Internet Protocol and related protocols.

General background on switching

The basic mechanisms of communications were long based on two very different sorts of technology. One is the broadcast technology of radio, wherein a signal is sent through free space and received at any point within the radius of the sender where the signal levels are high enough for the receiver to sensibly receive them. The other is the point-to-point communication of wired connections in which a wire that contains the signals being sent is connected to the sender and receiver and the communications sent through the wire from sender to receiver is effectively limited to that pair of parties.

13 Far more detailed coverage is provided in L. Duranti, “Diplomatics: New Uses for an Old Science”, Archivaria 28. 7-27, 1989. and L. Duranti, “Diplomatics”, Encyclopedia of Library and Information Sciences, Third Edition DOI: 10.1081/E-ELIS3-120043454, 2010, Taylor & Francis.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Broadcast communications have various problems like the mixing of signals from multiple sources, interference, reduction in signal strength with distance and intervening physical structures, and so forth. Point-to-point communications have various problems like only connecting one location to one other.

Line switching

In order to address limitations of point-to-point wired communications, line switching appeared in the early 20th century. Wire communications, like telephone lines, went from the business or home to central offices, where an operator, and eventually mechanical then electronic switching circuits, connected incoming 'lines' to other 'lines' to allow the same wires to be used to connect between arbitrary pairs of communicating parties. Local calls were connected directly, while long distance calls went through “trunk lines” from one switching center to another until they were connected over long distances with multiple operators or switching centers involved. Amplifiers were used en route to regain adequate signal strength against loss of signal over distance. Since the total number of wires in the switching center available to be connected to by calls was limited, calls were often not able to get through and thus a busy signal was associated with the lack of available lines, and a different busy signal was associated with the specific line being called already being in use by another call. These methods and the event sequences associated with them were the transmission protocols used for line switching systems.

Shared line signaling

In the days before the ARPAnet was created, there were various methods for switching sequences of signals between multiple lines so that the same physical line was shared. For example, there were the methods of time division and frequency division multiplexing. Frequency division multiplexing allowed different frequencies of signals to share the same physical line and be sent to different lines at central offices. Time division multiplexing allowed different “time slots” to be allocated to different communications over the same line. Equipment at central offices supported these methods and even allowed calls to be set up on different paths through different frequency and/or time allocations so that parties had 'virtual lines' from place to place that could be altered by changing the electronic configurations at the central offices. The provisioning of these virtual lines and the methods used to share lines constitute the transmission protocols used in these media and methods.

Message switching

The ARPAnet, and to a lesser extent other networks in the early 1970s, started to support a new approach to switching communications called “packet switching”. In the early days of the ARPAnet, “Interface Message Processors” (IMPs) were used to break communications into sequences of messages. Messages were “stored and forwarded” over multiple “hops” to get from one place to another with the IMPs storing messages until a time slot was available for the message to be forwarded on the proper line for the next hop of the journey from source to destination.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Messages went from IMP to IMP until they reached an IMP directly connected to the identified message destination, at which point they would be delivered. These “messages” necessarily had various formatting requirements so that the automation of the IMPs could figure out where to send them, and there were supporting sets of transmission protocols for allowing the design and implementation of mechanisms and messages so that they would interoperate properly.

One of the problems with this sort of infrastructure, and one of the key issues underlying the development of the ARPAnet, was reliability. Wires are very reliable in that, except for things that physically break or alter the physicality of the wires, they operate indefinitely always transmitting signals they receive from one location to another. More complex electronics breaks more often, requires maintenance, and requires continuous power supplied at many points. Unlike plain old telephone service (POTS) which gets its power from the central office, switched systems require more advanced technology on and between endpoints, and thus power becomes a more critical issue throughout.

In order to assure continuity of service even when parts of the overall network fail, the ARPAnet was designed to allow the paths messages took to automatically adapt over time and conditions. For example, IMPs were designed so that if one IMP failed, and if there remained another path from endpoint to endpoint, the remaining IMPs could adapt their routing of messages to take an alternative path. Similarly if there was network congestion, alternative paths could be taken for some of the messages to share the load across alternative paths. All of this operated in the ARPAnet of the 1970s and it was transparent and automatic to the users of the ARPAnet.

Packet switching in the ARPAnet and Internet

Many protocols were devised to allow things like breaking up larger messages into smaller “packets”, sending the packets out over multiple paths, and reassembling them at endpoints so as to increase bandwidth and reliability for the message. The Internet Protocol (IP) defines the sequences of bits exchanged between computers, and in particular, at the level of IP itself, defines a method for transmission and reception of IP “Datagrams.” Different sized packets were and still are used for different purposes, areas of packets were reserved for “headers” and “bodies”. Messages were used to encapsulate other messages, protocols were designed for transferring large numbers of files each in a long series of messages (e.g., file transfer protocol FTP), protocols were defined to support remote terminal sessions (i.e., transmission control protocol TCP), short messages were designed for use with commonly accessible endpoints called servers (e.g., domain name servers DNS) to support things like translating between human memorable names (e.g., all.net) and protocol addresses placed in message headers (e.g., addresses like 107.180.21.239), and different protocol layers were devised for layering logical messages (e.g., Internet datagrams) within physical messages (e.g., Ethernet packets). To support these various methods of encapsulation, coding, and transport efficiently, hardware-based packet switching devices have advanced to do far more complex tasks than the original IMPs did, but the basic functions remained the same:

1. Receive a packet and store it temporarily
2. Determine how to route the packet content based on the packet content, internal routing tables, associated algorithms, and other relevant data

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

3. When resources are available, transmit an appropriate outbound packet with the content to next 'hop' toward its destination.

Packet switching has come to dominate the communications industry as a method for data transmission and IP has come to dominate the format and protocol used to transmit information in packet switched networks. This is largely because it allows minimal connections from endpoints to switches and from switches to other switches, and so forth to form a hierarchy or mesh network that allows message traffic from anywhere to go to anywhere else by sharing the same physical connectivity.

But there is a price to pay for sharing the same communications lines and switching infrastructure, and that is the exhaustion of available resources. As more people try to send more packets through the same infrastructure at higher rates and more often, the total capacity of the infrastructure gets consumed and eventually can be overwhelmed. For that reason and others, there is a system of prioritization associated with packets. It is also well known that when lines are shared, one user might be able to examine the content sent between other users. Another price paid in shared communications infrastructure is that observing and/or altering traffic communicated over a shared line is feasible:

- Observing such traffic uses a process often called “sniffing” and it can be thought of like wiretapping. It is used for diagnostic, debugging, and other similar purposes, but can also be used for nefarious purposes.
- Injection or alteration can cause false transmissions including sending packets where they should not go, substituting packet content, potentially disrupting mechanisms at any level of operation, and deceiving parties to the communication.
- Encryption and authentication of network traffic is a way to reduce the effect and defend against observation and alteration of content in transit.

A commonly used term of art for sequences of packets being sent as part of a larger whole message or message sequence is a packet or traffic “flow”.

Gateways and firewalls

While the underlying infrastructure of the backbone of networks operated and still operate this way, at the edges, there were and still are a variety of mechanisms designed to accomplish other objectives. One of the most common mechanisms is called a “gateway”. A gateway is generally a mechanism that allows internal communications to operate internally in whatever manner that are designed to operate while still interacting with the Internet at large. The Internet follows IP which identifies formats for transmitted messages (called datagrams), but within connected networks, such as those used at universities, companies, in government, and elsewhere, completely different mechanisms, protocols, and formats might be used.

An example of this is the token ring architecture of the 1980s, first brought out by IBM, and eventually adopted as IEEE standard 802.5. Token ring attaches three bytes (a token) to the beginning of a message on a local area network and passes it from device to device around a “ring”. The three byte header identifies the token ring interface that is to receive the content, and all others simply pass the packet (containing the header and the message) to the next interface. The valid recipient consumes it and does not pass it along.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Token ring is a very different approach to networking than the hierarchical and mesh structure of the previously described routing and switching approach, it has different coding of headers and content, and it is not directly connectable to the Ethernet technology which has multiple endpoints connected to a local hub or switch to communicate. However, a gateway computer between the Ethernet and token ring technologies allows them to be connected so that different tokens in the token ring correspond to different IP addresses in the Internet delivered through the common Ethernet interface on the Gateway computer. The gateway does the translation by remembering the association between the two networks and rewriting the content into the proper formatted packets to support transit from interface to interface and thus network to network.

Gateways were, among other things, places where Internet traffic passed between internal and external networks. As such, they were considered an ideal location for checking the propriety of content entering and leaving the internal environment. This was implemented in gateways and as part of surrounding infrastructure. One widely recognized book on this area of security was published in 1994 and contained a chapter titled “Gateway Tools” detailing some of the tools and methods used in gateways as part of firewall technology at that time.[14] (herein [B&C]) This chapter of [B&C] also references Appendix A of [B&C] which lists free tools available at the time and cites papers from many years earlier.

The architecture of firewalls at that time included a gateway or router behind which there was a demilitarized zone (DMZ) with servers including a gateway, a filter bridge, and other such things. [B&C Figure 6.1 on p 129]. Many of these concepts and realizations involved multiple computers behind a router which intercepted traffic flows between external and internal resources and performed various kinds of security-related functions including logging, inspection, proxy services, and so forth. Many firewall architectures arose over the following years. I created and taught courses in firewalls in the late 1990s and early 2000s, including recording a course on the subject for use at the University of New Haven, slides for which were completed in 1999 and used to teach students at Sandia National Laboratories.[15]

In the late 1990s, TCP wrappers were one of the more interesting technologies freely available for use in firewalls and on servers. TCP wrappers were a tool devised specifically to allow blocking, passing, or rerouting of specific traffic based on various criteria. This allowed a wide range of security functions to be easily implemented in existing operating environments without otherwise changing those environments. Firewall ToolKit was also freely available at that time.

The Internet Protocol and Network Address Translation

There are different versions of the IP. The most commonly used one in the late 1990s and into the 2000s was version 4, often identified as IPv4. IPv4, among other things, used 4 8-bit bytes (called octets) to encode each IP address. 4 8-bit bytes is 32 bits, and as a result, there are only 2^{32} or 4,294,967,296 (~4.3 billion) unique IPv4 addresses. In the 1990s, it became widely understood that the total number of available IP addresses might be inadequate to handle all of the devices that might eventually be attached to the Internet. Indeed today there

14 Cheswick and Bellovin, “Firewalls and Internet Security – Repelling the Wily Hacker”, 1994 ISBN 0-201-63357-4, Addison Wesley

15 http://courses.all.net/Firewalls/index.html

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

are more than 1.6 billion Internet-connected phones in China alone. If the number of unique addresses run out, then there is no such address to assign to the next computer added. Also, if every address might appear anywhere at any time, the routing infrastructure must contain tables with routing details of all 4.3 billion devices and update them as they move around. This becomes too hard to manage. That's one of the reasons that today, IPv6[16] (with a 128 bit source and destination address, for 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses) is used in almost all cellular systems and many other Internet places.

A certain portion of IPv4 addresses are "reserved" for "local" use.[17] They are identified as not publicly routable and they should not be accepted or used in the Internet as a whole. They are available for any organization to use internally. Just as a gateway between token ring and the Internet can be used to translate internal and external addresses, the same sort of translation can be used between internal and external networks even if they are both running IP. This was widely used then as today to allow a change in external Internet Service Provider (ISP) which necessitates changes to external IP addresses to be made without renumbering of internal IP addresses.

If there are more internal computers than available external addresses, some computers will not be able to communicate with the Internet if there is a one to one mapping between internal and external addresses. Network Address Translation (NAT) allows one external address to communicate with many internal addresses through a translation process.

While NAT gateways existed earlier, in 1999, the Internet Assigned Number Authority published a detailing of how this mechanism worked.[18]

NAT is particularly useful in obfuscating the number and types of computers on one side from the other side of the NAT, and limiting activities so that the only transmissions that can reach the inside of the NAT are the result of an initiating transmission from the inside of the NAT. By using NAT between your home computers and the Internet, you prevent IPv4 traffic from entering unless as the results of a channel for flow opened by an internal device. However, IPv6 is designed to bypass all such controls, making it more dangerous and harder to control.

Commensurability[19]

Commensurability is required for content to be transmitted meaningfully. For example if I tell you "esdrfvok er098jr rfd coifr vg09nfb", unless you can find a way to translate this into a common language, you cannot reasonably be expected to understand it. Most coding schemes in computers are commensurable at the level of the symbol sets used, in the sense that every symbol in a digital computer is represented by one of two distinct values. But, just because there is a commonality of the bit level of using 1s and 0s to represent each symbol in every coding scheme, doesn't make the symbols across coding schemes commensurable.

16 https://datatracker.ietf.org/doc/html/rfc8200 and previously https://datatracker.ietf.org/doc/html/rfc2460

17 https://tools.ietf.org/rfc/rfc1597.txt downloaded for reference as rfc1597.txt it identifies as of 1994-03 "Address Allocation for Private Internets" including 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 - 192.168.255.255

18 https://tools.ietf.org/rfc/rfc2663.txt downloaded for reference as rfc2663.txt it identifies "NAT Terminology and Considerations", as of August 1999 and details how NAT works in gateways.

19 Defined in the Oxford Languages dictionary as: Measurable by the same standard.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

- Some symbol sets are from larger spaces than others, (e.g., 8 bit symbols of ASCII vs 32 bit symbols of UNICODE), which implies that there is no universal translation between them. Even though ASCII can always be turned into Unicode, of which ASCII is a subset, Unicode has symbols that just don't exist in ASCII. However, ASCII can be translated into UNICODE, which makes them partially commensurable because the common coding scheme that can be used to understand both is UNICODE.
- On the other hand, at the next level up the stack from 1s and 0s to symbol encoding schemes, sequences of symbols in different languages may not be commensurable because there is no commonality between them. For example, "esdrfvok er098jr rfd coifr vg09nfb" is not commensurable with any language currently existing because I just typed it in by pushing a bunch of keys on the keyboard with no information content (a.k.a. meaning) behind it.
- Human languages are typically only partially commensurable, and more generally, any human to human communication is only partially commensurable. In some sense, human language is an attempt to convey the thoughts in one mind to another mind. Since we all represent things at least a bit differently, even the most skilled writer and reader cannot perfectly communicate.
- Computer systems of similar types are able to communicate with excellent commensurability. For example, two computers exchanging date and time information using a standard time base can readily communicate time to each other, and the network time protocol[20] (NTP) is an example of a method by which this is done to set computer clocks to within milliseconds of each other worldwide.

Compatibility and interconnections

Similar devices using similar mechanisms and media for communication are usually reasonably compatible in the sense that communication between them is easily accomplished, predictably reliable or unreliable, timely, and commensurate, and so forth.

Additional problems start to arise as compatibility of components is less obvious and straight forward.

- **Translators between protocols (for messaging)** are commonly used. A most obvious example is the use of Web-based interfaces tor text messages. The Web interface communicates using the hypertext transport protocol[21] (HTTP), while text messages generally use the Short Message Service[22] (SMS) protocol. In most cases, the content is simply extracted from the old and then re-encapsulated into the new protocol. This is also done in various ways by proxy servers that rewrite incoming content for transmission to the next recipient.
- **Translators for content (for embedded languages)** is a more recent innovation in the networking space, and is increasingly used for real-time transcription into text, translation into other languages, and presentation to the user or vocalization by text to voice translation.

20 https://datatracker.ietf.org/doc/html/rfc5905 described at https://en.wikipedia.org/wiki/Network_Time_Protocol
21 https://www.rfc-editor.org/rfc/rfc9110.html – an Internet Standard also referencing earlier RFC versions.
22 https://en.wikipedia.org/wiki/SMS for descriptions and https://datatracker.ietf.org/doc/html/rfc5724 for details.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

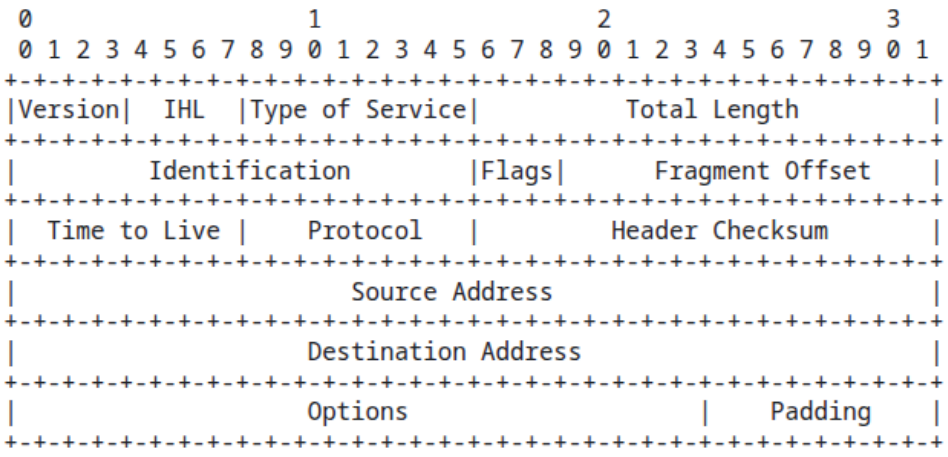
- Language translation has been performed in automated form since at least the 1970s as part of research, but there are substantial problems, particularly with idioms, ambiguities, and cultural differences that call for something more than word for word translations. This then goes to issues of meaning in context (see below).
- Today, there are also translators between computer languages, so for example, a program written in one language(e.g., javascript) is translated into another language (e.g., perl) or vice versa. These can be more precise, but today remain problematic.
- Many 'high level' computer languages are 'compiled' rather than being 'interpreted'. Interpreted languages are examined in real-time by another program that parses the syntax (sequences of symbols of the interpreted program) and implements the semantics (instruction sequences to be executed based on the parsed syntax in context). Compiled languages are parsed before run-time and translated into a 'lower level' language or other intermediate form before then being translated into the machine language of the system they operate in. In either case there is some level of translation required to turn the input syntax into the acts of the device.
- Human language is 'translated' from sounds into signals in the brain that people then use to interpret them. Dogs and other animals are trained to translate linguistic expressions into their behaviors, which are sequences of actions they have been trained to undertake in response to the linguistic expressions.

- **Recursive embedding and tunneling (encapsulation)** is often used in modern communications systems to encapsulate the desired message within an available protocol and communications media.
  - **The World Wide Web** (Web), as an example, operates over a set of encapsulated protocols, each acting as a container for the next. What you see on the screen is a rendering expressed in a language called Hypertext Markup Language (HTML)[23]. The language can be stored and communicated in any way, but the Web embeds HTML within the Hypertext Transport Protocol[24] (HTTP). HTTP is a protocol, so it is not stored, but rather communicated. While it can be communicated within other protocols, it is normally embedded within the transmission control protocol[25] (TCP) because TCP provides for separation of and later reassembly of the sequence of packets comprising a message, and it operates as a session between two endpoints for multiple exchanges of content over time. TCP can be embedded in different protocols as well, but in the Internet, it is normally embedded with the Internet Protocol (IP), either version 4 (IPv4) or version 6 (IPv6). IP is used to route packets from a source to a destination over the routing infrastructure of the Internet, allowing any embedded protocol, including TCP, but also other protocols, like user datagram protocol[26] (UDP), internet control protocol[27] (ICMP), and so forth, to communicate. IP is embedded in the local network protocol which controls the bits sent and received between devices on a local network segment.

23 https://www.ietf.org/rfc/rfc1866.txt
24 https://datatracker.ietf.org/doc/html/rfc2616
25 https://datatracker.ietf.org/doc/html/rfc9293
26 https://www.ietf.org/rfc/rfc768.txt
27 https://datatracker.ietf.org/doc/html/rfc792

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

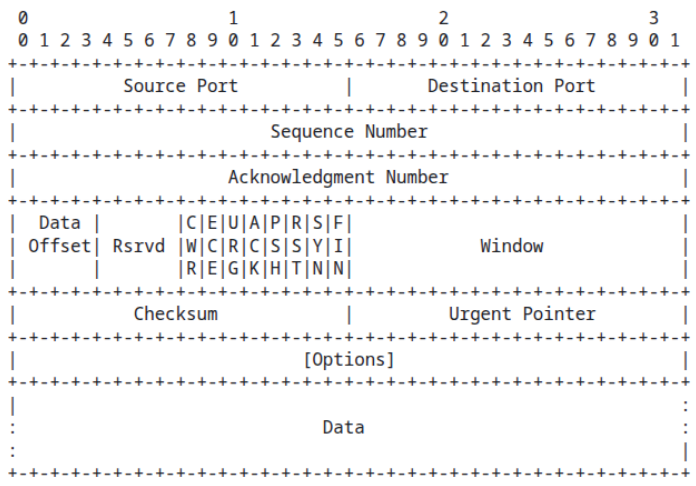
- The way this works, explicitly, is that IP contains an area called a header and an area I will call the data. The header provides a sequence of bytes indicating the source and destination IP addresses, the length of the datagram, and other data used for the protocol, and is followed by the body containing whatever sequence of bytes is to be delivered.[28]



Example Internet Datagram Header

Figure 4.

  - The data contains any embedded content associated with the embedded protocol, for example, the TCP protocol, which itself has a header followed by data:



Note that one tick mark represents one bit position.

Figure 1: TCP Header Format

    - Within the TCP data area, the HTTP protocol is embedded by placing the protocol elements in this data area.
      - Within the HTTP area, the HTML content is embedded, etc.

28 https://datatracker.ietf.org/doc/html/rfc791

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

- **Protocols within protocols** can also be used to whatever level desired, including recursively, within limits. For example, we can express Internet protocols within HTML by making the HTML content include sequences of symbols expressing HTTP within TCP within IPv6, and within that HTTP embedded in the outer HTTP, we can express HTML that describes DNS within UDP within IPv4, and so forth.
- **Limits of encapsulation** have to do with the available size of the next layer above the encapsulated content. While the mechanisms can split content across packets for later reassembly, the headers at the top level cannot be split, because the entire header and at least a few bytes of data must fit in the pentagram in order to be transported. However, that's not all that many bytes, and current networks support this without a problem. But as the level of embedding increases, more and more of the available packet size is dedicated to headers, leaving less and less bandwidth for the content.
- **Virtual Private Networks (VPNs)** are an example of embedding commonly used in the Internet today. VPNs usually embed IP within TCP within IP, with the TCP acting as a channel between two endpoints over long time frames. A connection is made between the endpoints using the relevant protocols, but then at each end of the connection, a program is run to make that endpoint act as if it were an IP address range routed separately from other routing on the computer. All IP datagrams routed to the designated IP addresses are routed through the VPN, embedding whatever else is sent. Many VPNs also encrypt all the traffic between the endpoints so that devices between only see the encrypted content, the location of devices on the other end of the connection are obfuscated appearing as if they were on the same network segment as the other devices on the local network, and the traffic pattern of the VPN is the mix of traffic patterns associated with all of the computers sending packets through the VPN.

- **Encryption and other intentional incompatibilities** create a communications channel with a lack of commensurability for those not intended to be participants. These are intentionally incompatible in the sense that some sort of common content or method is used to alter transmissions and reverse the process at reception. Some examples of this include:
  - Simple ciphers, like the Caesar cipher that changes A to C, B to D, and so forth.[29]
  - Modern encryption systems are far harder to defeat than most older methods.
  - Klingon is a made up language (aren't they all?) that emerged from the television show Star Trek. For those who cannot speak or understand it, it is a form of encoding messages to limit participants in the communication to those who know it.
  - Context-driven communication is often hard to understand without the context. For example, "Remember that thing we did at that place with the huge buildings? I saw 3 of them." Unless you know what the participants were talking about, the message is incompatible with your understanding, even though you can understand every word and understand the sentence. You just don't know what it refers to… means.

29 https://all.net/edu/curr/ip/Chap2.html within https://all.net/edu/curr/ip/index.html F. Cohen, "Introductory Information Protection", Chapter 2 - Cryptographic Protection

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

- **Indirect indicators and covert channels** exist in essentially all communications.
  - **An indirect indicator**, is for example, external information that might reveal the meaning or color it differently than the obvious interpretation. In putting together the puzzle, we can take external information and meld it with the content available in the observed communication to get more meaning. For example, if I know who the communicating parties are in the context-driven communication above, I can look up their travel records and other indicators of where they were when, identify places they were together (same place same time), identify which of those placed had big buildings, and narrow the search. Next we can, for example, look up the surveillance available there and then to see what they were doing to identify the thing they were doing in that place. If we then compare visuals from that place and time to those from the more recent locations of the speaker, we may identify just what they were communicating.
  - **Covert channels** are channels of communication not intended to be channels of communication. This usually includes things like timing and volume, power consumption, reflected light, and so forth. These include things discussed earlier under sensors. A good example is research done into keystroke timing and sounds.
    - It turns out that there are slightly different sounds associated with different keys on a keyboard. It also turns out that typing takes different times between different pairs of characters. By detecting the timing of keystrokes sent over a network, each sent within a single packet, the timing can be used to determine what is being typed, even if the content itself is encrypted.
    - By listening carefully to microphone input, the small differences in the sounds of different characters on a keyboard can be associated with the sounds sensed to determine what is being typed. This can be done, for example, using your smart phone to listen to the things you type into your computer.

  Workload may not justify the use of these methods in all situations, but they are available in essentially any communications environment. And of course, it's not just for keyboard entry. Covert channels exist in essentially all communications and the things we may understand from them vary widely. Body language showing interest otherwise hidden, behavioral twerks giving away what cards you are holding, scents indicating medical conditions or what you ate at your last meal, and on and on. And at every level of the ability to sense and every type of sensor method, there are covert channels and indirect indicators.

Appearances can be deceiving

This horrible example, acts consistently to undermine anyone looking closely over network telecommunications exchanges necessarily trusting. The reason it does this is that if you look at the first letter of each word, you get the real message. "The actual content" is different than the apparent content. As such, appearances can be deceiving. This particular example is a simple version of steganography, the placement of content within other content so as to hide the underlying message.[30] Content is hidden in pictures, movies, texts, and so forth.

30 https://en.wikipedia.org/wiki/Steganography

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Computerized communications deception

Similarly, things that look alike might not be the same. A “wolf in sheep's clothing” so to speak is an example of a classic tale about this, but today, technology supports all manner of “covert channels”[31], channels of communication not intended to be such. Examples include many of the items discussed earlier, like temperature leaks, sonic vibrations detected by visuals, and so forth. But they also include a wide range of detectable signals within computer systems and networks reflecting differences in the operating environment caused by detectable phenomena and effected in other detectable phenomena acting as sensors. When you use disk space in a shared storage system, it is not available to me. When you use network traffic in a shared infrastructure, my bandwidth may be effected.

Biological communications deception

Deceptive appearances are also used in the biological realm to send messages. For example, certain cephalopods change shape and color to signal other creatures that they are actually rocks or plants or other surrounding environmental objects. Cuttlefish are great examples of this.[32] They change shape using muscle and colors using “skin covered in millions of pixel-like cells called chromatophores: pigment-filled sacs each surrounded by their own small muscle fiber. These muscles can stretch the chromatophore to flood with color or contract and shrink to a dot, creating varied, complex patterns”. Other animals do this as well.[33] While you might not think of this as communication, it is exactly that; communicating to others in the environment that these creatures are different from what they really are.

Suppression and induction of signals

Deception in general can be thought of as suppression and induction of signals to cause differences between what is observed and what would otherwise be observed. It generally involves attacks on the cognitive system of the target of the deception, and can occur at any level of their cognitive processes. For now, we will focus on lower-level deceptions which cause the sensors of others in the environment to produce results that are interpreted by the limitations of low-level mechanisms of observers, such as changes in color and texture. But in general, this extends to higher levels of the cognitive system. [34] [35]

Interactions in the media

A key to understanding this in the context of this chapter is to recognize that communication is not only limited to the internals of the specific control system at issue, but that control systems interact with other control systems through the common environments they operate in. When multiple control systems are in place, the media they effect and observe don’t only interact with your control system, they interact with all the other control systems sharing the media or otherwise acting or or sensing it.

31 https://en.wikipedia.org/wiki/Covert_channel
32 https://www.nationalgeographic.com/animals/article/octopuses-squid-cuttlefish-cephalopod-camouflage-color-shape-changing
33 https://en.wikipedia.org/wiki/List_of_animals_that_can_change_color
34 http://all.net/journal/deception/index.html for further reading
35 http://all.net/books/Frauds.pdf for further reading

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

There are many examples of how this works, and in general, you can reasonably assume that every form of sensor and actuator may be causing and effected by these commonalities. So when we communicate sensory information to control mechanisms and control signals to actuators, that communication may interfere with or be interfered with by other control systems, intentionally or accidentally, randomly or systematically, and this can effect the control system's ability to act, just as signals in the media between system actuators and sensors can effect overall operations.

The extent of that interference in the communications realm is dependent on the physics of the media and the environment it interacts with, the signal transmission and processing mechanisms in use for the transmissions, and what is considered to be interference. By this last remark I mean to say that "interfere" is defined as "(1) take part or intervene in an activity without invitation or necessity, and (2) prevent (a process or activity) from continuing or being carried out properly."[36] If the only objective of the communications system is to accurately communicate signals from sensors to control mechanisms and control mechanisms to actuators, then covert channels that don't otherwise alter the control system activities are not interfering, and we normally don't care. But if the objective also includes not allowing others to observe or alter the information being transmitted, then covert channels might be a concern because they produce alterations even if they don't otherwise effect the control system operation. This gets more deeply into the issues of system objectives, and is covered later in this book.

Meaning in context

Information only has meaning in context. As such, the same information might mean different things in different contexts, and different information may mean the same thing in different contexts. Contexts are generally, the environment in which the communications take place. That includes, among other things:

- **The sources**: sources of information injecting signals into a communications media do so with intent or not, and with intent, the intent is to get content through to one or more destinations.
- **The intended destinations**: Intended destinations of communications typically have capabilities the source(s) intend to actuate, and this means they interpret the content in predictable ways. Thus the sources can encode their signals to convey the desired information to the intended destinations.
- **The other observers**: Other observers are anything other than the intended destinations that can observe the signals being transmitted. They may interpret the information in whatever way they may, and this may be very different from how the sources intended when encoding their transmissions.
- **The other actors**: Other actors may be inducing signals, changing the characteristics of the media, or doing anything else to induce meaning into the context of the communication.

Note please that I have anthropomorphized (acted like they were intentional beings) above to make things simpler.

36 Definitions from Oxford Languages Dictionary

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Obviously, by now, we don't have a real theory of meaning for sources and destinations of transmissions in control systems. And that is the point. Each mechanism does what it does with or without intent, and the control system that is successful is able to communicate signals to the level of precision and accuracy necessary to convey what was sensed and observed to the control mechanism and to convey what the control mechanism sent to the actuators. The success is determined by the effectiveness of the communications components in the context of the control system as a whole. In other words, meaning only makes sense in context.

- For a live creature, staying alive is the assumed meaning of a working control system.
- For a system with specifications, staying within the specified behaviors is the meaning.
- For an information theoretic communications system the symbols sent were received.
- For people, I understood what you meant to convey.
- For creatures communicating warnings or enticements, it's the responses of others.

Meaning is a function of context.

How much of what can I get through that channel?

At the level of bits, or 'symbols' in the sense of Shannon[37], the physicality of the system dictates the information content transmissible through a channel, and according to Shannon and Signal to Noise ratio results, it comes down to so many bits per second in the digital form, or so much bandwidth (as a frequency range) in the analog world.

- Bandwidth is an expression of the range of frequencies for transmission, or in other words, the width in frequency range from the lowest frequency to the highest frequency of the transmission. If a signal is sent over a frequency range of 20-520 cycles per second, the frequency range is 500 cycles per second, and any frequency in that range can be used to express a different value. As an analog value range, there are an infinite number of different frequencies in the range, but the ability to differentiate them for transmission and reception is typically limited. The amplitude of signal can also be used, and again, the range of transmittable amplitudes may vary continuously over a range, but the ability to differentiate them by sender and receiver limits their actual utility for sending different information.
- The information content of a message (expressed as H(x) for a message x in base 2 for bits) is the number of bits of content of the message. This is expressed based on the statistical frequency of the symbols composing the message in the context of the language and the actual symbols being sent. A simple coding for a sample language with 3 symbols (A, B, and C) and A has a 50% likelihood while B and C each have a 25% likelihood, would potentially code A as [0], B a [10], and C as [11]. To express ABCAAACAB, we would write the sequence as 0101100011010 ([0][10][11][0][0][0][11][0][10]). For 9 symbols it took 13 bits, but on average, it takes 1 bit for A (50% of the time) and 2 bits for each of B and C (25% of the time each), or 50%*1+25%*2+25%*2, or 0.5+0.5+0.5, or 1.5 bits per symbol. If the probability was ¼ for each of 4 symbols it would take 2 bits per symbol, but for ABCD at 50%, 25%, 12.5%, and 12.5%, it could code as [0][10][110][111] or 1*0.5+2*0.25+3*0.125+3*0.125 or 1.75 bits per symbol.

37 C. Shannon, "A Mathematical Theory of Communications", Bell Systems Technical Journal, 1949.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

Once we add the additional layers on top of the mathematics and physics, it's not so much the quantity as the quality that counts: how much meaning we can transmit, how much of what importance we can transmit, and how much we can effect the desired outcome by what we transmit. And of course, this is a function of context. If someone is injured, a single bit of information is all that's needed to trigger an emergency response, if the system is designed to operate that way. For example, if an emergency always starts with the bit value '1' and all other communications start with a bit value '0', it takes one bit for emergencies and more than one for anything else. This is also the concept underlying compression. For example, Huffman codes use statistics of characters (symbols) used in a language (e.g., English) and assigns different codes of different lengths for different characters based on their frequency. The most common symbols are sent using the smallest code lengths while less common symbols are sent with longer code lengths, so that on average, communication is more efficient than simply assigning each symbol a different bit sequence, all of the same length.[38]

Of course what we choose for symbols sets the coding, and that sets the information content of the message. For example, if we used words from a limited dictionary, call each word a symbol, and optimized the coding of those symbols, we might get much better compression, and be able to express more information in the same channel. Information only has meaning in context. Someone watching the same channel with a different dictionary would have problems making sense of the messages.

In many control systems today, the protocols used to exchange information between a Supervisory Control and Data Acquisition (SCADA) system and a Programmable Logic Controller (PLC) express data values to place in or retrieved from registers of the PLC. But without knowing what actuators and sensors are associated with each register and how the overall system operates, these values are meaningless. The same value in the same register could mean the water level in a tank, the temperature in a blast furnace, the extension of a ladder, or anything else. Information only has meaning in context.

Back to compatibility

In addition to the message sender and recipient using compatible symbol sets and coding, there is also the compatibility between components of the composite. Sensors and actuators operate in whatever form the media may take, atomic, chemical, biological, optical, sonic, or whatever. But when mixed in the communications to a control system, there has to be some translation into the symbol sets or frequency ranges, or whatever the media is for the communication, and between that media and the control mechanism. And those have to be compatible or made compatible by additional components. A biological sensor connected to a radio frequency communications media, connecting to a digital computer, sending signals through fiber optics to a speaker that operates underwater means some sort of bio-to-electromagnetic mechanism, electromagnetic to digital mechanism, digital to optical mechanism, and optical to vibration mechanism. These are implemented with various techniques to translate analog to digital, digital to analog, chemical to electrical, electrical to mechanical, and other similar compatibility mechanisms. And each of these has operating limitations, ranges, characteristics, and so forth. Composites of compatible components are built up by having additional components to make overall systems operate.

38 https://all.net/edu/curr/ip/Chap2-1.html goes into details about various aspects of these issues. For a more complete picture, see https://all.net/edu/curr/ip/index.html which is about information protection generally.

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved

The academic field of communications vs. this chapter

It would be premature to complete the discussion of communications without mentioning the academic field of the same name.[39]

> "Communication studies (or communication science) is an academic discipline that deals with processes of human communication and behavior, patterns of communication in interpersonal relationships, social interactions and communication in different cultures" (as cited in the reference)

However, as you can see from our discussion, this sort of communication takes place at a higher level involving the concept of cognition, and is beyond the scope of this part of this book, which addresses components of control systems and the mechanics of transmission of content from place to place in a purely mechanistic manner.

And yet, even at this rudimentary level, we can see the foundations of cognitive limitations and interpretation based on the limitations of control systems associated with the richness of reality vs. the ability to communicate within and between sensors, actuators, and control mechanisms.

We see what we want to see and hear what we want to hear… starts at the sensors, and continues to narrow through the communications mechanisms and architecture, and into the meaning of content being based on its context.

39 https://en.wikipedia.org/wiki/Communication_studies

 Copyright (c) Fred Cohen, 2025 - All Rights Reserved