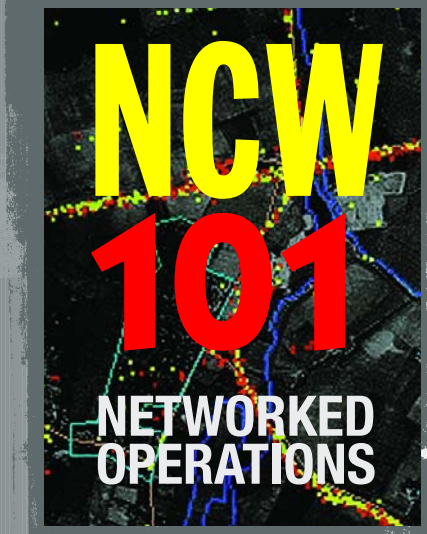

$7.95
Defence today
DEFENCE CAPABILITIES MAGAZINE
STRIKE PUBLICATIONS
Abrams M1A1
ready for
urban ops?
Maritime warfare
in the littorals
NCW
101
NETWORKED
OPERATIONS
Wedgetail
concept
of
operations
Smart tankers hub in network
Print Post PP424022/00254
ISSN 14470446
02
9 771447 044001



Network Centric Warfare Fundamentals

Part 2

Dr Carlo Kopp

Digital datalinks and networks

Digital datalinks exhibit the technology at the heart of modern wireless networks, and thus are also the technological basis of systems supporting Network Centric Warfare and Network Enabled Operations. Despite the pivotal importance of datalinks, and networks, the technological issues central to these areas are not well understood outside the relatively narrow communities of scientists and engineers who develop and support the technologies. In a sense this should not come as a surprise since the technologies are inherently complex. However, understanding fundamental issues does not require high-level qualifications – and this NCW 101 Part II aims to explore the basics in datalinks and networks.

In the simplest of terms, a digital datalink is the wireless equivalent of a modem used to communicate over a cable. Early digital datalinks emerged during the 1950s and 1960s and often by design differed little from voiceband modems used for communication over telephone lines.

The simplest possible voiceband modem running over a telephone line emits a tone that is modulated to carry a stream of digital data – effectively transmitting either '1' or '0' at any given time. Very simple modulation schemes such as Frequency Shift Keying (FSK) increases or decreases the pitch of the transmitted tone depending on whether a digital '1' or '0' is being sent. The modem at the other end of the link recognises the changing tone and demodulates the traffic to produce a stream of digital data - '1' or '0' in digital form.

A simple (or 'dumb') modem of this type does not interpret the stream of digital data it is carrying, or the structure of the digital data. The next step in modem evolution was the incorporation of a digital interface, capable of understanding the digital format and buffering it.

Radio datalinks of comparable complexity did not differ significantly from voiceband modems. Rather than impose the digital modulation onto a voiceband carrier wave, they employ a radio frequency carrier. In effect, a basic radio datalink transceiver differs little from a voice radio of the same generation: rather than using circuits to impose voice modulation, and extract voice modulation in the receiver, a 'modem-like' digital modulator and demodulator were used. Datalinks permitted direct communications between computers, which previously had to be sent by voice, and a human operator would then type the message into the computer.

The earliest operational datalink systems, adopted during the 1960s, were used primarily to feed target coordinates from ground-based radar tracking systems into the fire control computers of interceptor aircraft. This was the era of the Cold War, where interceptors were the primary defence against nuclear-armed bombers, and the timelines during an intercept were critical to success. Having a computer on the ground with direct interceptors saved critical minutes or seconds.

The basic measure of performance for any digital communications system is its throughput, measured in 'bits/second', or the amount of data that can be transferred over a link per second. It is limited by the parameters of the radio modulation being used for the link.

Configuring computers to communicate reliably is not a trivial task. Synchronisation of messages is critical to success: both machines need to understand what is being sent across the link, and what to do with it. Reliability also becomes an issue as radio transmissions can degrade or drop out for a variety of reasons, or be jammed by opponents.

The next step in the technological chain was the adoption of 'protocols' for machine-to-machine communications. A protocol is a set of defined rules, and defined data formats, understood by both computers at either end of the link. A protocol provides a framework for formatting and sending digital messages, and a framework for receiving and understanding digital messages. Protocols define the exact format of messages being transmitted, and will usually keep track of what was sent should a message be lost enroute, and automatically (and transparently) retransmit the message.

One of the first platforms to deploy the new JTRS terminals will be US Air Force tankers, as tankers are ubiquitous in the battlespace and thus provide persistent presence.

Datalinks emerged in strength during the Cold War to support interceptors tasked with destroying nuclear armed strategic bombers.

Much of the enormous growth in digital communications since the 1960s, and in computer networking, has happened as a result of maturity in protocol technology. While we have seen more sophisticated digital modulation schemes appear since the 1960s, nearly all were understood theoretically during that period. A good example is COFDM used in HDTV, digital stereo and high speed wireless networks devised during the late 1960s but too expensive and bulky to use then.

Datalinks considered today as 'legacy systems' remain in wide use for a range of applications. Examples include: Link 1, which runs at 1200/2400 bits per second; TADIL A/Link 11/11B which runs at 1364 bits per second; TADIL C / Link 4, which runs at 5,000 bits per second; and Link 14. Each of these systems has a defined protocol and a defined radio modulation technique.

Assessment of the capabilities of any datalink needs to look at several key issues:

1. Security of transmission - can the link be easily eavesdropped, and can it be easily decrypted by an opponent? From an operational perspective, security is critical. The case study of Allied intercepts of the German Enigma system illustrates the point that knowing an opponent's every move apriori provides an enormous advantage in combat. Technological measures adopted to provide security in datalinks are manifold and encryption techniques to encode transmitted data are a science in their own right. Modulation techniques designed to be difficult to detect and demodulate are another.
2. Robustness of transmission - can the link resist the effects of solar flares, bad weather, terrain and hostile jamming?

Robustness is no less important, as even if an opponent's messages cannot be decoded, shutting them down can be almost as useful. Nature can be almost as capricious as an opponent, and this must be managed. High robustness is achieved by choices in link modulation, transmitted power levels, but also in protocol design, to allow retransmissions until the message can get through.

3. Transmission capacity or throughput - how much data can the link carry per second? Throughput is becoming increasingly important, as operators demand the capability to send large blocks of reconnaissance imagery, or observe live video feeds of surveilled targets. The price to be paid for throughput is in more complex modulation schemes and protocols, more expensive hardware that usually emits more power, and in an increasing demand for scarce radio frequency spectrum availability. With a plethora of commercial terrestrial and satellite services occupying useful radio bands, radio spectrum availability and demand for throughput can collide.
4. Communications protocol compatibility - how many systems can understand the message formats being used? The issue of protocol compatibility has been a headache since the 1960s, and arguably will always be. The problem revolves around two issues: platforms and systems equipped with wholly incompatible datalinks, and datalink implementations that are only partly compatible. The latter is the more insidious, as datalink equipment that is nominally compatible may differ in detail, to the extent that some message types will simply not be understood. The result is that the platforms or systems using such partially compatible datalinks may have only a fraction of the functionality expected.

In perspective, point-to-point datalinks will remain with us for some time to come. Other than supporting legacy systems, dedicated datalinks will continue to be introduced for unique or special applications where the simplicity of a point-to-point link permits early deployment.

Networks vs Datalinks?

The next step-up in the technological hierarchy are networks. Networks take the idea of the datalink one step further, permitting computers to communicate with many other computers, rather than only a single sibling.

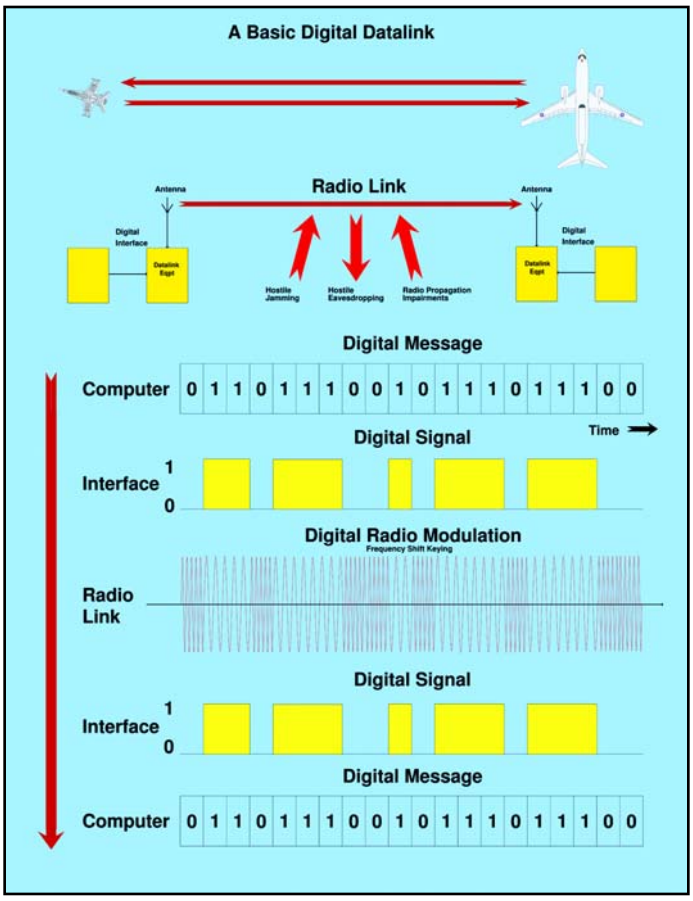
At the basic functional level, networks are mostly systems in which messages can be sent between arbitrary computers within the system, all sharing some common datalink scheme and protocol.

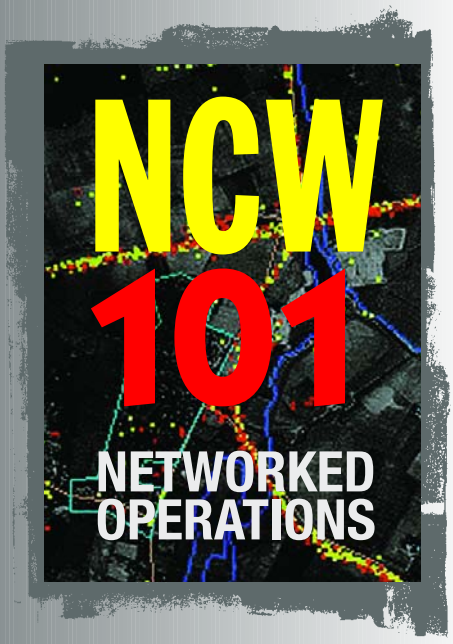
The ability to send messages to multiple recipients, or gather messages from many senders, is where much of the power of networking lies. Commercial networks are primarily divided by their geographical footprint into local area networks, which span areas of kilometres in extent, and wide area networks, which may be citywide, nationwide or global. While local area networks may share a common channel, in practice most networks are divided into smaller chunks, and messages are routed between these 'subnets' whenever they need to cross a local network boundary.

The idea of routing is powerful, as it allows local network traffic to be confined and thus not congest other parts of the network. Congestion remains one of the ongoing issues with all networks, a byproduct of many computers competing for limited capacity on the network.

One of the most important differences between basic datalink protocols and networking protocols is that the latter require a proper addressing mechanism to identify computers connected to the network. A dedicated datalink may not require any addressing - the choice of radio channel (frequency) may be enough to distinguish the systems sharing the channel. Conversely, in a network with dozens, hundreds, thousands or even millions of systems, addressing becomes a critical issue.

It is important to note that networks are in effect aggregations of datalink connections, but use protocols designed for a networking environment where large numbers of computers must be uniquely identifiable. Many of the issues that arise with datalinks remain as issues with networks, since the physics and mathematical premise remain largely the same.





The US Army is placing heavy reliance on the new JTRS WNW protocol to provide connectivity between land force assets.

Measures of Network Capability

Like datalinks, networks can be compared through their basic design parameters. The four basic issues that apply to datalinks also apply to networks:

1. Security of transmission
2. Robustness of transmission
3. Transmission capacity or throughput
4. Communications protocol compatibility

However, networks must by design and function also address other design problems:

Address space - how many computers (systems) can be uniquely identified in the network?

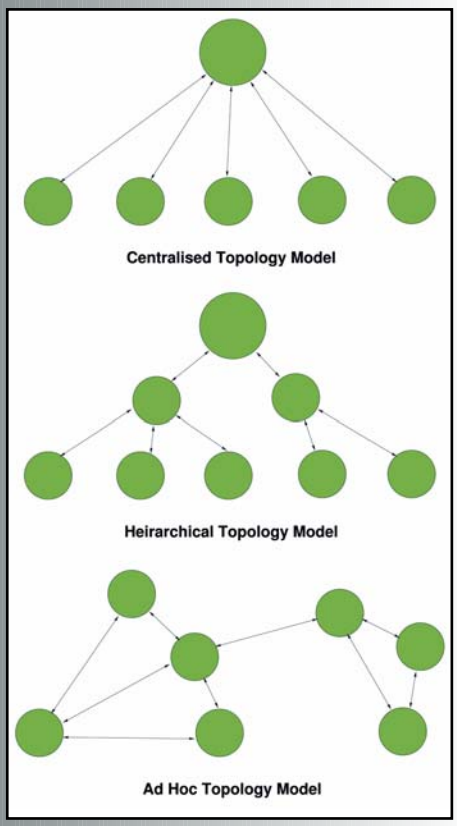
Limitations in address space are what led to the adoption of the IPv6 protocol, over the current IPv4, within the Internet. Running out of addresses puts hard limits on the size of any network, and ultimately its geographical extent.

Congestion management - how does the network cope with peaks in traffic load?

One of the realities of the networking world is that traffic load varies over time, and in periods of peak activity congestion may occur, as a result of which throughput can be impaired or traffic discarded. At the least, the network will slow down over load and time critical traffic may be delayed. Unwanted delays can actually disrupt the function of many network protocols, especially those carrying time sensitive traffic like digitised voice or video streams.

Topology model and traffic routing - how is the network interconnected and how does this impact network capabilities?

Network topologies are a byproduct of the basic design of the network, and reflect the realities of a shared communications channel, with many users contending for the channel. Good choices in topology cope well with localised disruption or congestion, poor choices do not.



A special case in network topology is the Ad Hoc Network, now emerging in the new US JTRS network protocol. Ad Hoc Networks are self-forming and the topology depends on which platforms participating in the network can immediately provide connectivity to other platforms in the network. The most common topology models of interest today are the centralised model (JTIDS/MIDS is a variant), the hierarchical model (Internet) and the ad hoc model (JTRS, MANET).

It is important that networks be compared or assessed against all of these cardinal parameters. Not every network design is well adapted for every environment, and this must be considered in planning for new networks.

Evolution of Datalinks and Networks

The evolutionary process leading up to today's menagerie of datalinks and networks occurred in part because the military experience mirrors the commercial domain, but also lags it by at least a decade. There are important differences between the commercial and military networking worlds: military networks rely heavily on wireless links while commercial networks rely more on copper/fibre cabled links; and military networks have to assume hostile action, especially jamming and eavesdropping, commercial networks much less so.

The key caveat is that both worlds progressed from a complex mix of specialised and proprietary single purpose datalinks, and then networks, which have progressively been displaced by common and shared standards. Given the significant cost in retrofitting hundreds or thousands of datalink and networking terminals across equipment fleets, the rate of change in the military domain has been much slower than in the commercial domain. Replacing a $100 networking card in a desktop computer is trivial in costs against integrating a $250,000 JTIDS terminal in a military jet.

A quick summary illustrates this evolutionary process convincingly:

1. Link 1 datalink at 1200/2400 bits per second used for air defence systems, devised and introduced in the 1950s.
2. TADIL A / Link 11/11B datalink at 1364 bits per second, used for naval links and ground based SAM systems using original CLEW DQPSK modulation or newer FTBCB convolutional coding at 1800 bits per second. It is 1960s technology.
3. TADIL C / Link 4 datalink at 5,000 bits per second in the UHF band, used for naval aviation, AEW&C to fighter links, and fighter to fighter links on the F-14 series. It is also 1960s technology.
4. Link 14 datalink used for HF transmission between naval combatants at low data rates.
5. TADIL J / MIDS/JTIDS / Link 16 network, which is a jam resistant L-band time division spread spectrum system based on 1970s technology. This system is the dominant 'standard' at this time.
6. Army Tactical Data Link 1 - ATDL 1 used for Hawk and Patriot SAM batteries.
7. PATRIOT Digital Information Link - PADIL used by Patriot SAM batteries.
8. Tactical Information Broadcast System - TIBS used for theatre missile defence systems.
9. PLRS/EPLRS/SADL are a family of US Army/Marine Corps datalinks used for tracking ground force units, and providing defacto Identification Friend Foe of ground units. EPRLs is also used for data transmission between ground units.
10. CDL/TCDL/HIDL/ABIT are US high-speed datalinks designed primarily for satellite and UAV transmission of imagery. CDL family links are typically assymetric, using a 200 kilobit/s uplink for control and management, and a 10.71, 45, 137 or 234 Megabit/s high speed uplink, and a specialised for the control of satellite/UAVs and receipt of gathered data. ABIT is a development of CDL operating at 548 Megabits/s with low probability of intercept capabilities.
11. Improved Data Modem (IDM) is used over Have Quick II spread spectrum radios to provide low data rate but secure transmission of targeting coordinates and imagery. It has been used widely for transmission of targeting data to F-15E/F-16C strike fighters and F-16CJ Wild Weasels. It is essentially an analogue to commercial voiceband modems.
12. TCP/IP (Internet) protocol implementations running over other channels.
13. JTRS (Joint Tactical Radio System), including the WNW (Wideband Networking Waveform), and TTNT (Tactical Targeting Network Technology) protocols. JTRS is in development and intended to replace JTIDS with a faster and more flexible system. Initial JTRS terminals will include interfaces to support most legacy protocols in use, and JTRS will have the capability to carry TCP/IP traffic. The JTRS system sits at the leading edge of this evolutionary process, whereas the mature JTIDS/MIDS is in the process of large-scale deployment in the US, while the earlier legacy protocols are being progressively phased out over time.

In operational terms, the network of most interest in the near term is JTIDS/MIDS, since it is available and is now used by the US often as a defacto IFF system. In terms of fixed infrastructure facilities, the TCP/IP network is of most interest.

The reality for the ADF is that as JTIDS reaches significant penetration across the ADF equipment fleet, JTRS will be deploying across the US fleet. As a result, the ADF should be positioning now to acquire JTRS terminals for key assets, such as Wedgetail, planned UAVs and other ISR systems.

Comparing Networking Models

To best appreciate the strengths and limitations of the three leading network technologies in use, it is illustrative to compare the basic models used. The TCP/IP network protocol suite dominates Australian commercial markets, and fixed Defence infrastructure. It is designed to run over a cable infrastructure, and its wireless extensions are not well adapted for military use, due to poor jam resistance and security mechanism designs.

TCP/IP networks are mostly hierarchical in topology. As a result, such networks are vulnerable to disruption or destruction of key nodes or links in the network, typically those that aggregate traffic from large numbers of smaller networks. Another weakness in TCP/IP is limited security, essentially an artifact of its evolution from a DARPA/NSF funded network for interconnecting academic, industry and defence computers in the US. As a result, it was implicitly assumed that computers connected to the Internet would be operated by cooperative and well behaved users. The reality of today's commercialised Internet, flooded with spam and XXX rated websites, indicates the unintended consequences of mixing technology designed for a secure environment with the uglier realities of the commercial world.

JTIDS was devised during the 1970s primarily to support air defence operations with a jam resistant datalink, capable of supporting large numbers of fighters and missile batteries in the high density European theatre. While JTIDS is today largely referred to as network, in strictly technical terms it is more the shared datalink channel than the network.

JTIDS uses spread spectrum radio frequency modulation techniques for its signal, designed to resist significant levels of jamming (a future NCW 101 article will explore spread spectrum techniques in more detail). Unlike conventional 'point to point' datalinks, JTIDS uses a technique called 'time division multiplexing' to share the available spectrum between hundreds of terminals. These may communicate with other terminals within the immediate footprint of the network, more recently a relay capability has been added to permit multiple JTIDS networks to interconnect.

Because the timing pulses and synchronisation of a JTIDS 'network' are centrally controlled, JTIDS in a sense uses a centralised topology model, and where the central node, such as a warship or surveillance aircraft, routes traffic between JTIDS users, this is unambiguously the case.

In a high intensity combat environment, any central node upon which the whole network depends becomes a single point of failure if it is disabled or destroyed. In this respect the JTIDS model has a weakness, and this needs to be carefully addressed in operational planning.

The JTRS WNW is to use ad hoc networking protocols, in which any entity participating in the network will route traffic for any other entity, as required. Ad hoc networking systems are topologically the best choice for military applications as there is no single point of failure in the network. Ad hoc networks are self-forming and self-healing, as no participating terminal is topologically 'above' any other. The difficulty with ad hoc networking is that it is immature, and many aspects of ad hoc network design remain in development.

In conclusion, the basic ideas underpinning modern digital networks are not complex, but the technology required to build them is.

Further reading:
http://www.ausairpower.net/isr-ncw.html
http://www.csse.monash.edu.au/~carlo/adhoc.html

The US Army is a major user of various point-to-point datalinks, used to provide connectivity between components of air defence missile batteries.

Part 3 next issue .. JTIDS in detail