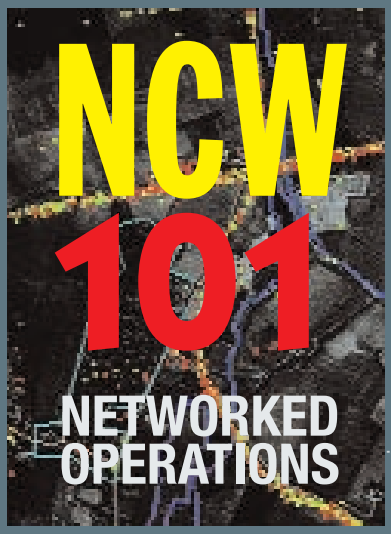


Network Centric Warfare Fundamentals

Part 3

Dr Carlo Kopp

JTIDS / MIDS

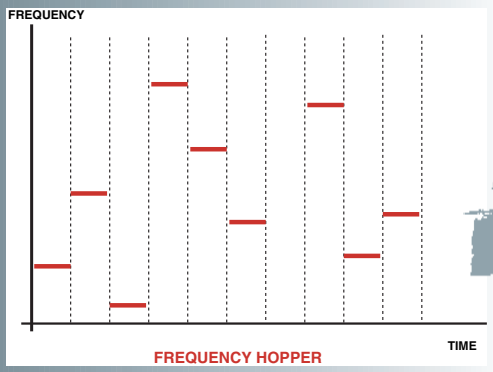
The Joint Tactical Information Distribution System (JTIDS) network, and its evolved offspring MIDS (Multifunction Information Distribution System), form the defacto standard military digital network in use today – dominating military network installations in the coming decade until its planned replacement, the Joint Tactical Radio System (JTRS), finishes development and is deployed in sufficient numbers to matter.

Contrary to commonly held belief, JTIDS/MIDS is not new technology, even if many current production terminal equipments are recently designed. The JTIDS modulations and protocols were devised during the 1970s in the US and NATO countries, using a combination of modulation technique invented in 1942, error correction coding invented in 1960, and a timesharing technique of similar vintage.

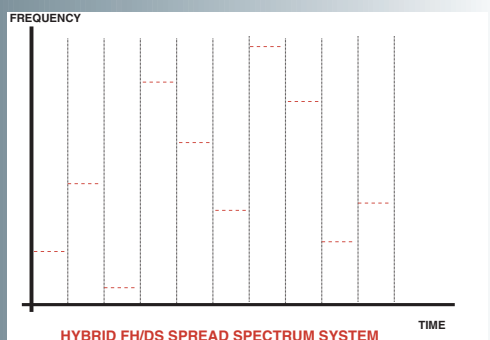
JTIDS/MIDS is also a limited networking scheme in terms of coverage footprint and achievable network capacity or throughput. It's architecture initially aimed to provide situational awareness data and targeting data in air defence operations, and this has constrained its utility in a number of ways.

These limitations aside, JTIDS/MIDS provides valuable capabilities, many of which have never been seen before. Perhaps the most important of these include transparency, the ability to network assets without significant operator intervention, and ubiquity (the ability to connect air, land and sea assets seamlessly).

To gain a good picture of the strengths and limitations of JTIDS/MIDS, we need to explore three aspects of the design. The first is how it encodes and protects data, the second how it addresses individual network terminals, and the third the geometrical constraints on its coverage. Inevitably many of its design features overlap these three aspects, which has historically been a cause of much confusion in the uninitiated.



FREQUENCY HOPPER



HYBRID FH/DS SPREAD SPECTRUM SYSTEM
(JOINT TACTICAL INFORMATION DISTRIBUTION SYSTEM)

How JTIDS/MIDS carries data

JTIDS/MIDS is what is termed a 'Spread Spectrum Multiple Access' system, as it uses spread spectrum radio techniques and provides a mechanism for multiple terminal access. This simple language conceals considerable complexity. Spread spectrum modulation techniques were invented by Hollywood actress Hedy Lamarr and musician George Antheil in 1942 (U.S patent 2,292,387) who discovered the technique while using a player piano to control frequency hops, but did not achieve prominence until the middle of the Cold War, as the complexity of such designs made them expensive to build.

There are two basic categories of spread spectrum techniques, and both are used in JTIDS/MIDS.

Frequency hopping spread spectrum techniques were the first to be introduced and the most widely used in military communications.

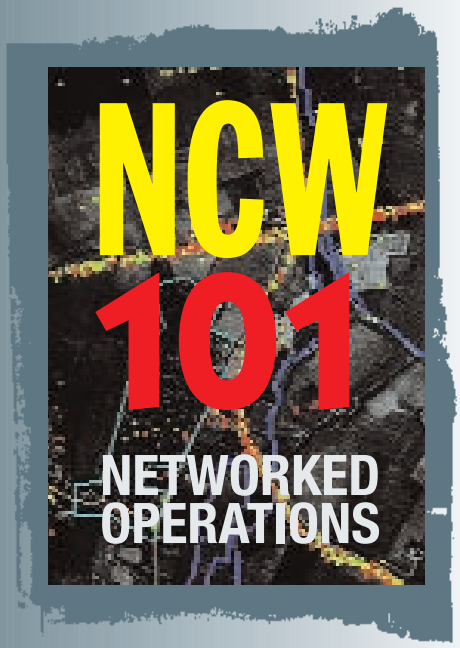
The basic idea underpinning all frequency hopping radios is that the frequency or wavelength of the radio carrier wave continuously hops around over time. Typically, a pseudo-random coding scheme is used to determine the next frequency to which the carrier wave should hop. Unless a receiver knows where the next hop will be, it cannot capture the signal and decode it. A hostile intercept receiver sees a carrier wave popping up and disappearing continuously over time, within some range of frequencies unique to the radio design.

Frequency hopping is used since it is very effective at frustrating hostile radio jammers. In a conventional radio scheme, the carrier wave sits constantly at some operating frequency and a hostile jammer can be easily tuned in to interfere with it. As the pseudo-random hopping code is kept secret, only authorised receivers knowing that code can anticipate where the frequency hopper will hop to next. Without this knowledge the jammer is frustrated.

Because radio waves travel at the finite speed of light, a frequency hopper that hops quickly creates much difficulty for a hostile jammer. By the time the hopped signal has propagated from its source to the jammer, it is apt to have hopped again to a different operating frequency. The jammer is thus forced to play a futile game of catch up.

There is a price to pay for the increased jam resistance of the frequency hopper. Because the frequency hopper only uses a small fraction of the available radio bandwidth at any time, the amount of data it can carry is reduced accordingly. A rough measure is that a tenfold improvement in jam resistance is paid for by a tenfold reduction in data throughput.

Frequency hoppers are not immune to jamming, but force up the cost of jamming equipment considerably since the jammer has to emit a jamming signal in each or most of the frequency slots the frequency hopper jumps between. In effect, an opponent has to maintain a battery of jammers to straddle much of the frequency range the frequency hopper operates in. Ten times as much jam power means a ten times bigger jamming system.

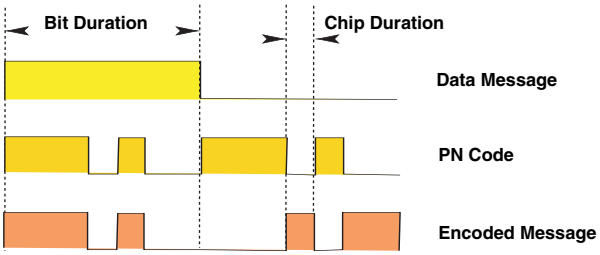


The second spread spectrum technique used is termed 'direct spreading'. It is simpler than frequency hopping and is also widely used. In a direct spreading design each digital '1' or '0' transmitted is replaced by a pseudo-random string of '1's or '0's. Unless a receiver knows what the pseudo-random encoded string is apriori, it has no means of knowing whether the data sent is a digital '1' or '0'.

Like frequency hoppers, direct spreading systems can have good resistance to jamming. The rough measure is that jam resistance is improved by a ratio equal to the number of '1' or '0' transitions in the pseudo-random sequence used to encode the direct spreading message. As with frequency hoppers, the price to be paid is a reduction of achievable data throughput per radio bandwidth, in proportion to the length of the pseudo-random spreading code.

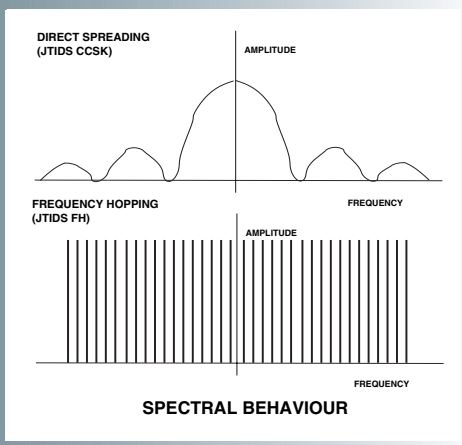
As an example, a conventional radio using 100 MHz of radio bandwidth might carry 150 Megabits/sec of data, but can be easily jammed by a hostile signal of similar strength. A spread spectrum radio, which uses the same 100 MHz of radio spectrum, might only carry 1 Megabit/sec of data, but can cope with nearly 100 times more hostile jamming power before it gets into difficulty.

In summary, spread spectrum techniques can provide vastly better jam resistance than conventional digital radio links, but per given radio bandwidth pay for this in a proportionate reduction in how much data they can carry. Spread spectrum radios can be intercepted only if the opponent knows what pseudo-random spreading codes are being used.



DIRECT SPREADING (DS)

Spread spectrum techniques have another interesting feature also exploited in JTIDS/MIDS. This feature is contingent on the mathematical properties of the pseudo-random codes being used. If these codes have a property called 'orthogonality', where a mathematical operation called 'correlation' between any two codes produces a result of zero, then two or more spread spectrum radios can operate within the same bandwidth at the same time. Each radio sees its peer's signals as little more than background noise.



SPECTRAL BEHAVIOUR

Again there is a price to be paid. This is because the jam resistance is reduced in proportion to the number of spread spectrum radios with unique codes sharing the same radio bandwidth. As always there are no free lunches in this game.

The baseline JTIDS/MIDS system hops at around 77,000 times per second. Each hop puts it into one of 51 radio frequency slots, each separated by 3 MegaHertz. The slots are fixed in the L-band, shared with IFF secondary radar signals, starting at 969 MegaHertz and ending at 1206 MegaHertz. Two blind 'notches' are excluded to allow IFF to share the radio bandwidth.

Within each hop of the baseline JTIDS/MIDS system, the signal is further encoded by way of direct spreading techniques, using a specific method termed Cyclic Code Shift Keying (CCSK). This second layer of 'spreading' converts 5 bits of raw digital data into a 32-bit pseudo-random sequence, transmitted in a short 6.4 microsecond 'pulse' (effectively a tiny burst transmission).

Frequency Number	Frequency (MHz)	Frequency Number	Frequency (MHz)	Frequency Number	Frequency (MHz)
0	969	17	1062	34	1158
1	972	18	1065	35	1161
2	975	19	1113	36	1164
3	978	20	1116	37	1167
4	981	21	1119	38	1170
5	984	22	1122	39	1173
6	987	23	1125	40	1176
7	990	24	1128	41	1179
8	993	25	1131	42	1182
9	996	26	1134	43	1185
10	999	27	1137	44	1188
11	1002	28	1140	45	1191
12	1005	29	1143	46	1194
13	1008	30	1146	47	1197
14	1053	31	1149	48	1200
15	1056	32	1152	49	1203
16	1059	33	1155	50	1206

JTIDS Frequencies. JTIDS hops between a total of 51 seperate frequencies (US Navy).

Without knowing both of these pseudo-random spreading codes an opponent can neither intercept the signal nor retune a jammer quickly enough to jam efficiently.

If we look at the baseline JTIDS/MIDS system in perspective, it is transmitting tiny 5-bit chunks of data 77,000 times per second, these chunks each encoded pseudo-randomly and hopped between 51 different radio frequencies pseudo-randomly.

It is this mechanism that provides JTIDS/MIDS networks with good jam resistance and reasonably good security.

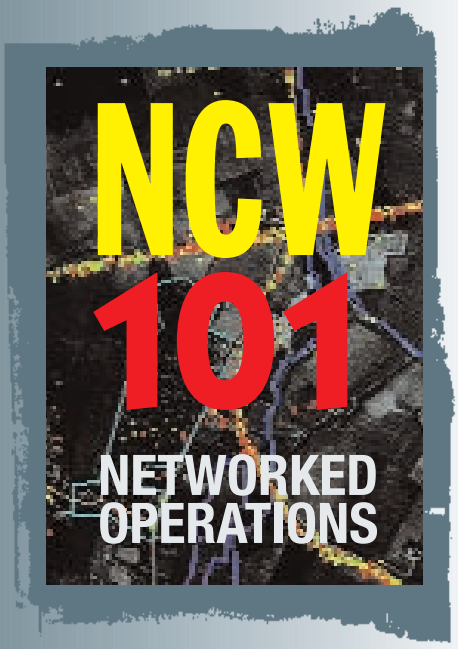
How JTIDS/MIDS addresses stations

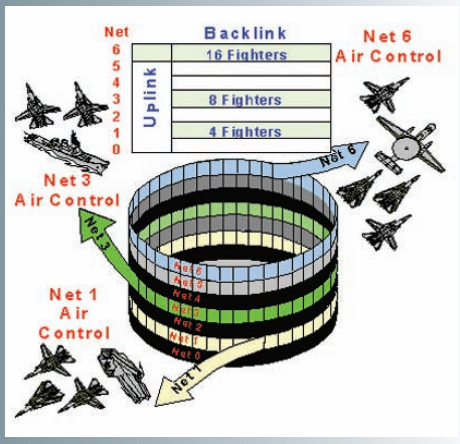
The JTIDS/MIDS system provides a shared channel between numerous stations. To allow stations to share the channel and be able to uniquely address each other, another mechanism is required. This mechanism is termed Time Division Multiple Access (TDMA), and has been widely used in commercial digital communications since the 1960s.

TDMA schemes rely on the idea of dividing time into a large number of typically identical time slots. Each specific channel to be carried is then allocated its own time slot. When that time slot comes up, a transmission is sent and received by the pair of stations sharing the slot. All stations each take their turn, according to the preprogrammed slot allocation. The rest of the time both stations do nothing, waiting for their slot to arrive. These schemes are inherently 'cyclic', in that, the sequence of slot allocations repeats again and again. If the rate at which these repetitions occurs is fast enough, a user communicating through a channel using time slots in this system simply sees a channel that can carry however many bits per second of data.

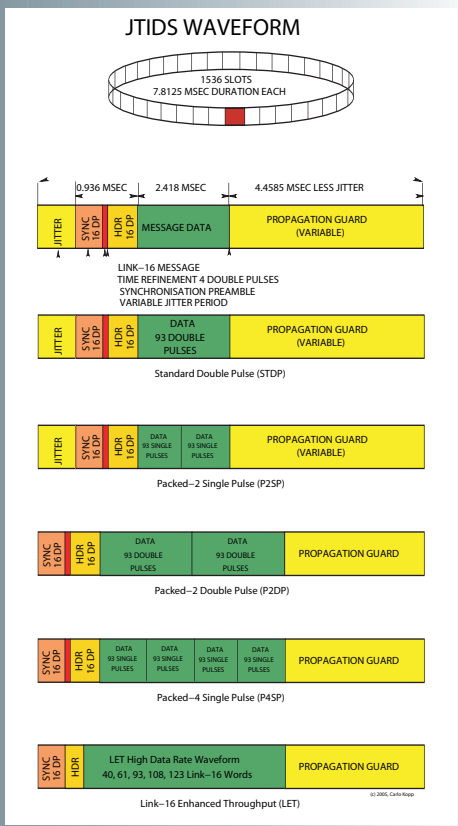
All TDMA schemes must have a protocol that defines when time slots start and stop, and who can use which time slot. Without such a protocol, chaos would be inevitable.

In the baseline JTIDS/MIDS system a twelve second cycle is used, divided into 1536 individual time slots. Each time slot thus has 7.8125-millisecond duration.





(US Navy Image)



Within each of these time slots a JTIDS/MIDS station transmits multiple pulses each of 5-bits of data. The standard specifies either 72, 258 or 444 pulses per time slot. Each of the 6.4 microsecond duration pulses is separated in time by at most 6.6 microseconds.

What this means in practical terms is that each slot permits the transmission of a chunk of raw data of between 360 and 2220 bits in size every 7.8125 milliseconds, for a raw data transfer rate between 46.08 kilobits/sec and 284,160 kilobits/sec. That data rate is shared between all of the stations participating in the network.

Why the gaps between pulses, and why the sedate cyclic rate for the times slots. This reflects several realities. The first is that the JTIDS design was conceived to support interceptors orbiting over Germany intended to stop waves of Soviet fighters. Updating each interceptor with threat data once every twelve seconds is a reasonable worst-case number. The gaps between pulses were set to reflect 1970s receiver designs, which require finite time to hop frequencies, and to minimise the time available to jammers. If you are hopping frequencies every 13 microseconds and transmitting for only 6.4 microseconds, a jammer must be at a distance of much less than 2 km if it is to have any hope of jamming the tail of each pulse, having detected the beginning of the pulse.

JTIDS/MIDS however uses a third mechanism to cause grief to opponents, although it is not always used. If we assume a pulse every 13 microseconds, and no more than 444 pulses per each 7.8125 millisecond time slot, we find a visible discrepancy in the numbers. Only 5.8 milliseconds are being used for actual transmission (3.354 for 258 pulses and 0.9 for 72 pulses), against a slot duration of 7.8125 milliseconds.

The remaining time is there to provide a time allowance for the radio signal to propagate to all stations in the network, and to allow intentional random jittering of the time at which the transmission starts in order to further confuse eavesdroppers.

The minimum time available for propagation and jittering is 2 milliseconds, during which the signal can travel 315 nautical miles less jitter time. In practice, a JTIDS/MIDS footprint of around 300 NMI is assumed.

The JTIDS/MIDS system is a good example of a layered approach to resisting hostile jammers, carefully melded with a relatively conventional TDMA scheme for sharing bandwidth.

Because of the type of pseudo-random codes used, the JTIDS/MIDS system allows 128 unique hopping codes. If more than one of these codes is in use at the same time, the network is said to be 'stacked'; it is concurrently operating between two sets of network terminals and sharing the bandwidth between them. The technique of 'stacking nets' is widely used but can often result in reduced throughput since the degradation in the effective noise floor (see above) can result in increased data transmission error rates.

When 'stacking nets' the cited limit is usually 20 concurrent hopping patterns before error rates produce significant impact. In the presence of jamming this will inevitably be reduced. If we assume each MIDS/JTIDS net is carrying data at 54 kilobits/sec (STDP see below), then stacking 20 x 54 kilobits/sec yields and aggregate capacity of about 1 Megabits/sec. For comparison, a single digital TV channel with MPEG encoding consumes twice that capacity.

Up to this point we have simply explored the mechanisms JTIDS/MIDS uses to create a transparent digital pipe between stations. What is being sent through that pipe adds further functionality, and complexity, to the system.

The Link-16/TADIL-J messaging format

Like most modern digital communications protocols, the Link-16 protocol transmits data in discrete and tightly defined chunks, termed messages. Each of these messages contains a data 'payload' and additional bits to facilitate its use. While the data payload is the useful content, the system cannot function without the other components of the message.

The JTIDS system has seen ongoing evolution of its message formats. Early JTIDS Class I terminals fitted to E-3A AWACS and F-15C fighters used a message format called Interim JTIDS Message Format (IJMS), which has been superceded in later Class II terminals with the full Link-16 message format defined in the US Mil-Std-6016 standard. TADIL-J is a US Navy designation, Link-16 US Air Force and NATO. Typically, only later US Air Force terminals are compatible with both the IJMS and Link-16 message formats.

Link-16 messages come in a variety of formats. The essential tradeoff is the data throughput versus jam resistance. Message packing formats that carry less data have better jam resistance.

All Link-16 messages share some common features, an essential byproduct of the need to synchronise receivers in terminals and to uniquely address terminals.

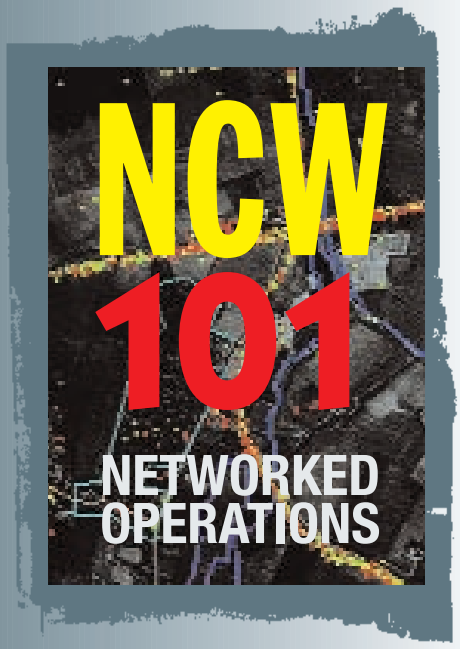
The basic structure of all Link-16 messages is that of a block of 36 synchronisation and header double pulses followed by the actual message payload. The 16 double pulses allocated to the synchronisation function allow a receiver to lock on to the JTIDS transmission prior to demodulating and decoding the transmission. The 16 double pulses comprising the header contain information that identifies the message. An additional four double pulses are included to allow control of timing.

The actual payload then contains either digital data for transmission between computers using the link, digitally encoded voice communications, or a unique message for Round Trip Timing (RTT). The system can also add redundant data to protect the message from bursts of transmission errors, typically as a result of hostile jamming.

This Error Detection And Correction (EDAC) mechanism uses Reed-Solomon (R-S) 15/31 encoding which provides the ability to correct up to 50 per cent of the encoded data if it is corrupted in transit. This is achieved at the cost of committing 31 bits of message to carry only 15 bits of actual content. Yet again jam resistance is improved, but at the cost of halving throughput. Voice channels do not use R-S EDAC capability. It is worth observing that Reed-Solomon coding is the basic technology used in CD and DVD data protection.

The payload is made up of chunks of data termed Link-16 words, each of which contains 70 bits of data and 5 parity bits for protection. All Link 16 messages are made up of integer multiples of Link-16 words.

There are four basic Link-16 message formats used. Some of these transmit every data pulse



twice to achieve 100 per cent redundancy for improved jam resistance, but also to compensate for propagation problems (for technical readers: CCSK is considered susceptible to multi-path interference) or antenna coverage limitations in manoeuvring platforms.

The Standard Double Pulse (STDP) message format has the lowest throughput but best jam resistance. It is typically used to carry three or six 70-bit Link-16 words, permitting each slot to carry 210 or 420 bits of data.

The Packed-2 Single Pulse (P2SP) message format doubles throughput compared with the STDP format, but does so at the loss of jam resistance provided by redundant double pulse transmission. It carries six 70-bit Link-16 words per slot.

The Packed-2 Double Pulse (P2DP) message format doubles throughput compared with the STDP format, but sacrifices the jitter capability, again at the expense of jam resistance. It also carries six 70-bit Link-16 words per slot.

The best throughput is provided by the Packed-4 Single Pulse (P4SP) message format, which has the weakest jam resistance, as the double pulse redundancy and jitter are not used.

These message formats determine how much data is sent in each time slot. They do not define what data is sent; that is defined by the message type.

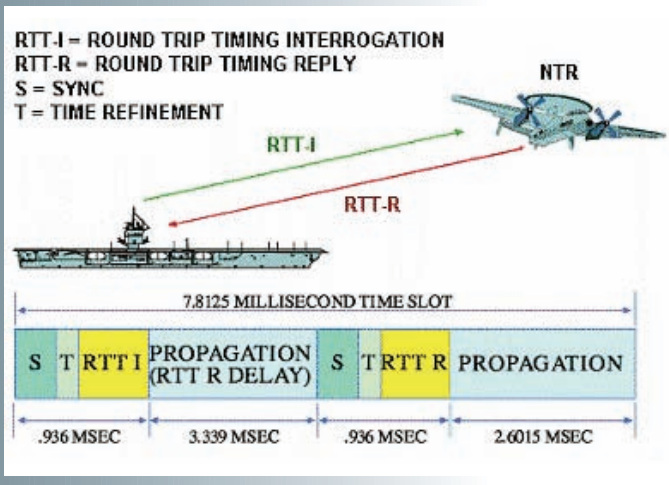
Link-16 message types

Link-16 is characteristic of modern military datalink designs, in that, it uses many dedicated message types for specific purposes, in addition to voice channel capabilities.

The Precise Participant Location Identification (PPLI) message type is widely used and a good example. This message type contains mission unit identification (JTIDS Unit (JU), IFF codes, unit type, mission identifiers, platform location and platform velocities, navigation accuracy, and datalink status.

The Round Trip Timing (RTT) message type is used to maintain timing synchronisation between JTIDS terminals in a network. RTT-I interrogation messages are usually generated by platforms that have difficulty synchronising; an RTT-R response message is then sent by a platform with more accurate timing to enable synchronisation to be corrected.

Each JTIDS terminal can support two digitised voice channels, termed "Voice Group A" and "Voice Group B". Typically these channels are stacked on different nets. This message type uses 930 bits in each slot for digitised voice.



(US Navy Image)

The MIDS/JTIDS system uses encryption techniques to protect payloads. Crypto variables (numbers) are used to select the pseudo-random frequency-hopping pattern, the jitter time, and the spreading pattern for each pulse. Additional crypto variables are used to encode the message payloads. Terminals have the architecture to permit cryptographic separation between nets being used concurrently.

JTIDS access methods

While MIDS/JTIDS is a time division multiplex system, in which timeslots are allocated to individual users for data or voice transfers, the system requires further enhancement to permit more flexibility in an environment where many user terminals may need access. In comparison, commercial TDM systems typically lack this capability and are designed with quite rigid schemes for allocation of slots.

MIDS/JTIDS timeslots are typically reserved as Transmit, Receive or Relay Transmit slots. A terminal cannot transmit in a slot reserved as a Receive Slot.

There are four most commonly used Access Methods in typical MIDS/JTIDS networks.

The Dedicated access method allows only a specific terminal to transmit in a designated slot and all others are only allowed to receive in this slot. A tanker aircraft broadcasting its location and fuel state might use the Dedicated Access Mode, while fighters would listen in this slot to monitor the tanker.

The Dedicated With Time Slot Re-use access method is similar to the Dedicated Access Mode, but allows a commander to reallocate the specific slot to a particular terminal.

The Contention Access Method mode allows all terminals to transmit in a so designated slot. If a 'collision' occurs when two terminals try to access the slot simultaneously, then the terminal with the more powerful signal wins.

The Push-To-Talk (PTT) access method is used for voice channels. Stations will not access the slot until it is vacant and no other terminal is transmitting in it.

Limitations and strengths of JTIDS/MIDS/Link-16

JTIDS/MIDS/Link-16 provides tremendous flexibility and has proven to be very useful operationally. The US now uses it largely as a substitute for classical IFF in combat. A number of weapon datalinks recently trialled have been built as derivatives of JTIDS, using unique message formats but retaining the modulation scheme.

Of all of the established datalinks, JTIDS/MIDS/Link-16 is usually regarded to be the most jam resistant. The combination of frequency hopping, CCSK direct spreading, message random jittering, double pulse redundancy and Reed-Solomon coding essentially defeats simpler jamming techniques and requires a combination of high jam power, large jamming bandwidth and smart modulation to produce serious jamming effect.

JTIDS/MIDS/Link-16 is not however without its limitations and problems. The limited data throughput is inherent in its basic architecture, which makes it ill suited to the transmission of bulk data such as ISR imagery or live video feeds. This constrains its usage to situational awareness functions, command and control, low data rate ISR functions, and derivative functions such as weapon guidance. In the long term it is likely to remain used for these purposes.

A second key limitation is that it is not well adapted to carrying 'bursty' computer traffic, as its ability to rapidly reallocate slots is limited. This is another inherent limitation of TDM systems and not one easily changed.
The third key limitation is its complexity, which drives up demands for skill levels in managing networks. While a user of a terminal might get by with training, which covers modes and message formats, personnel who are required to configure and manage networks require extensive and deep training to be proficient – especially in environments where jamming is expected.
Another issue frequently identified as a problem is a propensity for overly enthusiastic use of net stacking resulting in transmission errors and unreliability. This in part relates to the previous limitation and the inherent issues when performing multiplexing of spread spectrum channels. Every time an additional net is stacked, some jam resistance is lost, as the noise floor seen by platforms operating at the edge of the network pushes them closer to viable operating limits.
While JTIDS/MIDS/Link-16 is often seen as a panacea, it is not, and using it successfully requires considerable insight into its idiosyncrasies

JTIDS/MIDS/Link-16 terminals

A detailed survey of JTIDS/MIDS/Link-16 terminal equipment is a theme in its own right.
Early JTIDS terminals were prohibitively expensive, limited to IJMS format messages, often bulky and used only for key platforms. The more recent high volume production MIDS Low Volume Terminal (MIDS-LVT) is much cheaper and more compact.
Designed for use across a wide range of platforms, especially aircraft, a typical MIDS-LVT terminal is designed as a 'swap-out' form factor replacement for existing TACAN terminals, retaining an embedded TACAN transceiver as an option to cut integration costs, as the MIDS-LVT terminal can reuse existing power, cooling, antennas and cabling. It requires a Mil-Std-1553B or other connection to the central mission computer, and local machine software to access the network. Typical hardware costs for this class of terminal are around $250,000 per terminal, with around $250,000 per platform in software code to access the terminal. Additional software integration costs may arise. Putting MIDS-LVT terminals into 35 aircraft thus costs of the order of $20 million, or about $600,000 per aircraft.
Some estimates cited in Australia for network integration have been ridiculously high, suggesting that the actual costs of JTIDS/MIDS/Link-16 terminal integration are not widely understood.

The future

The long term US plan is to replace MIDS/JTIDS terminals over time with the new Joint Tactical Radio System (JTRS or 'jitters'), which will exploit newer technologies such as ad hoc networking. JTRS remains in development and delays have affected early production of the basic equipment.
In the mean time, some enhancements are being introduced to MIDS/JTIDS to alleviate - but not solve - problems arising from its basic design.
The Timeslot Reallocation (TSR) method is an additional Access Method (see above) which attempts to automate reallocation of available timeslots depending on immediate demand. What TSR does, via software enhancements in terminals, is to allow terminals to advertise their immediate demand for network capacity to all other terminals, upon which an algorithm in software in used to determine how many each terminal can actually get.
Another enhancement is the Link-16 Enhanced Throughput (LET) capability developed by Viasat in the US – intended to increase throughput. An LET capable terminal can communicate with non-LET capable terminals, but not vice versa in LET mode.
LET works by replacing the spread spectrum and Reed-Solomon encoding with a newer Reed-Solomon/Convolutional coding scheme, which can adapt to required link capacity. LET can provide 3.33, 5.08, 7.75, 9.0 and 10.25 times more throughput than the basic JTIDS modulation, but it does so at the expense of both jam resistance and transmission range. The fastest LET mode may be unusable in many combat environments.
Finally, encroachment into the JTIDS/MIDS portion of the L-band spectrum by civil operators will force the introduction of a 'frequency remapping' capability in future terminals, where the 51 hop frequencies are remapped to avoid the frequencies used by civil operators.

Part 4 next issue ..