Battlespace Communications Connectivity Model

ABSTRACT

A Battlespace Communications Connectivity Model was developed based on four domains – Core Network, Extended Backbone, Access Network and Peer-to-Peer Network. The model allows a battlespace communications grid to be synthesised from the most appropriate communications subsystems from each of the four respective domains into an integrated network to enable Integrated Knowledge-based Command and Control.

Seah Peng Hwee
Wong Choon Bong

Battlespace Communications Connectivity Model

INTRODUCTION

The world of communications connectivity is a complex one. From the plain old telephone service to the broadband wireless networks, from high frequency systems to software defined radios, from submarine cables to satellite links, there are many choices. To support the military's communications needs, the engineer needs to be conversant in the myriad of technologies available and plan intelligently for an integrated solution, which often involves a technology mix.

The skills for systems integration can be nurtured, and the Battlespace Communications Connectivity Model provides the systems thinking that enables such innovation. The model is an internal teaching aid used in project team discussions to propose alternative solutions to meet operational requirements. It was developed some years ago to facilitate the understanding of the various physical communications media subsystems that enable the deployment of an integrated battlespace communications infrastructure.

CHARACTERISTICS OF THE MODEL

The design considerations of the Battespace Communications Connectivity Model are summed up by four 'S's.

- **Simplicity.** The model must be logical and intuitive. It should recognise the laws of physics, such as the wave propagation characteristics in different frequency bands and the limitations of various channel modulation techniques. As an independent reference model, it does not make reference to any country-specific military communications architecture and is vendor independent. As it is founded on basic principles of telecommunications infrastructure, any military communications big picture or architecture can be broken down to fit the model.

- **System of Systems**. Each communication medium has its strengths and limitations. There is no one-size-fits-all communications solution. Therefore, a solution typically involves a combination of subsystems. This system of systems approach is essential in ensuring cost effectiveness when providing end-to-end solutions to military users in an integrated battlespace communications grid.

- **Scalability.** The framework must allow the individual domains to remain independent of one another. This facilitates technology management by allowing flexibility in the research, development and deployment of solutions in each of the domains. It is the responsibility of the system integrator and the technical architecture governance body to ensure interoperability between the different domains.

- **Survivability.** Communications technology has been evolving – networks are getting more resilient; information pipes are getting bigger; mobile solutions are getting more reliable; services are converging. To ensure unbiased evaluation of all possible solutions, the model should be independent of specific technologies. This will ensure that the model will not become obsolete over time.

THE MODEL DEFINED

When defining the Battlespace Communications Connectivity Model, various perspectives need to be considered.

- Topology – point-to-point, multi-point, star and mesh
- Deployment – strategic, operational and tactical
- Echelons – Brigade and Below, Battalion and Below, etc.
- Range coverage – personal area, local area and wide area
- Frequency band – Very High Frequency (VHF), Ultra High Frequency (UHF), microwave, etc.
- Wave propagation mode – Non Line Of Sight, Line Of Sight and Beyond Line Of Sight
- Data rates – narrowband, wideband and broadband

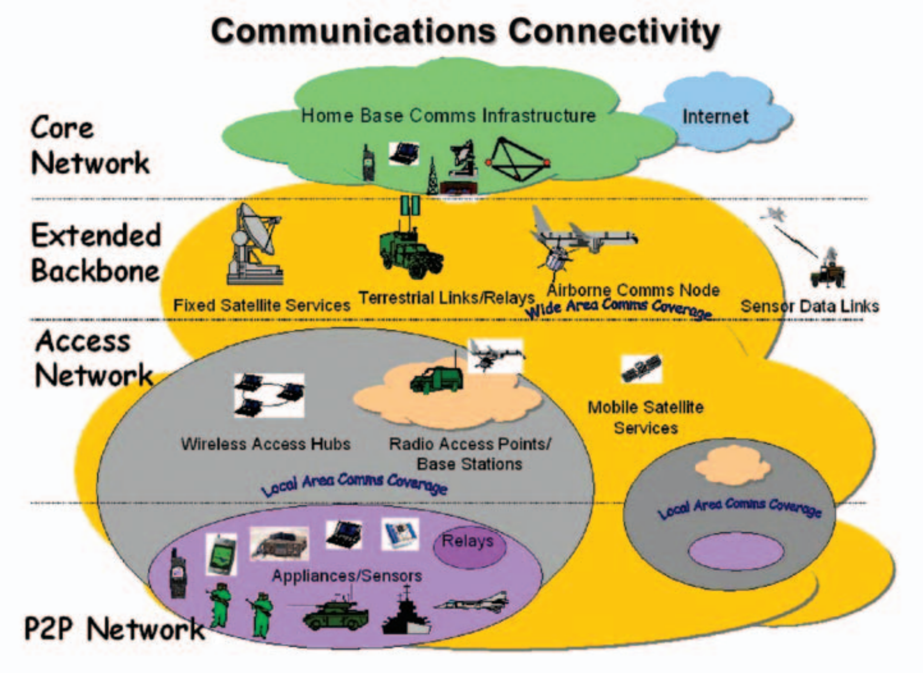

Figure 1: Battlespace Communications Connectivity model

- Mobility – static, communications-on-the-halt and communications-on-the-move

The proposed Communications Connectivity Model is based on a combination of the different perspectives. Founded on the principles of telecommunications infrastructure, it is all encompassing and lends itself readily to construct the communications grid for the battlespace. Readers are encouraged to consider the model from multiple perspectives.

In mirroring the commercial telecommunications world, the military communications connectivity model is developed based on four independent non-hierarchical domains. As shown in Figure 1, the four domains are the Core Network, the Extended Backbone, the Access Network and the Peer-to-Peer Network. In the homeland, communications and network infrastructure (both wired and wireless) are fixed. However, in the battlespace, communications infrastructure has to be set up in highly flexible and dynamic situations. Hence, other than the Core Network, the military communications infrastructure is normally dependent on wireless communications. It is noted that many military operations do not require all four connectivity domains to be present.

Core Network

The Core Network refers to the customised wired and wireless communications infrastructure in the homeland. This includes data networks, voice and line switching networks, transmission networks and access networks. It rides on the telephone companies' ubiquitous civilian infrastructure, with customised configurations for information security and redundancies for survivability. The core network is thus self-sufficient and complete within the homeland.

The Core Network is characterised by relatively low cost per unit of information transmission and access, as compared to other domains. Higher data bandwidth and better quality of service provide the basis for certain applications such as video streaming that users in the Access and the Peer-to-Peer Networks will be envious of. The challenges for the Core Network are the data bandwidth required for mobile broadband multi-media applications, routing survivability and access security.

The Core Network family consists primarily of the civilian infrastructure with examples including radio and line switches, Public Switched Telephone Networks, Wireless Local Area Networks (WLAN), Private Mobile Radio (PMR) networks and the public mobile wireless telephony cellular networks (such as GSM and 3G).

Extended Backbone

The Extended Backbone network is a wireless extension of the Core Network to the battle-space for reach-forward and reach-back operations. It also provides the reach-between among tactical forces deployed in the battlespace with distance separation.

The Extended Backbone is characterised as a long haul, high bandwidth, Beyond Line Of Sight communications link. It can stretch from tens of kilometres to halfway round the globe, depending on where the area of operation lies. The challenges for the Extended Backbone are the robustness of the wideband connectivity, its supportability, interference immunity and mobility, as well as the high costs of investment and operations.

The Extended Backbone family consists of technologies such as satellite communications (SATCOM) systems, troposcatter systems, Trunk Communications System (TCS), surrogate satellites on Unmanned Aerial Vehicles or High Altitude Platforms, and point-to-point sensor data links.

Access Network

The tactical Access Network allows individual communication appliances and terminals to be wirelessly connected to a base station (or hub) within its local range coverage. If the Access Network is in turn also connected to the Extended Backbone, then the appliances can be connected to a remote destination in the battlespace or homeland.

Bringing along a base station to the battlespace is tantamount to setting up a communications infrastructure necessary for the dependent terminals to work. Careful considerations need to be weighed in comparing the Access Network against the Peer-to-Peer Network in determining the best solution for each operational scenario. The Access Network provides a relatively bigger area of coverage within a more stable network. Challenges for the Access Network include access bandwidth and interference immunity.

The tactical Access Network is normally built on commercial technology, customised for the battlefield. Some examples are GSM/3G cellular networks, Trunked Radio Systems, WLANs, Bluetooth and Worldwide Interoperability for Microwave Access (WiMAX) systems. Commercial satellite communication terminals (e.g., Broadband Global Area Network) are also possibilities for less sensitive information, allowing connectivity to remote locations bypassing the Extended Backbone.

Peer-to-Peer Network

The Peer-to-Peer Network refers to wireless group communication among two or more compatible communication appliances and terminals without the aid of an intermediary infrastructure such as a base station. The challenges for such networks include the size, weight and battery-life of the wireless terminals, interoperability among devices, bandwidth limitations, and access security.

Appliances are what the military users use and see (i.e., soldier-centric). They hide the complex layers of the communications infrastructure supporting them. They include a whole gamut of end user communications terminals, devices and communicators: digital radios, computers, smart phones, hybrid PDA-phones, etc. Command and Control (C2) applications can also reside in certain appliances and access the network for contents and services.

Mobile Ad hoc Networks (MANET) is a key force multiplier in the P2P Network. Such networks are popular for military applications because they do not require any prior infrastructure set-up, which makes them ideal for rapid deployment. The network consists of an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organise themselves arbitrarily.

The P2P Network family includes military solutions such as High Frequency (HF) radios, VHF/UHF Combat Net Radios (CNR), Data Links (e.g., Link 16) and Software Defined Radios. Commercial solutions such as mesh WLAN are also popular.

END-TO-END SOLUTION – INTEGRATING THE PARTS

Media Gateways

To harmonise the diverse communications protocols and waveforms, communication routers or media gateways are needed at the central nodes, such as Command Posts, to interface different radio systems. They will interconnect the different communications media terminals (e.g., between CNR networks and TCS), which operate over different frequency bands and modulation techniques. Software defined radios will greatly simplify this problem. Media gateways are also needed as interface between SAF communications systems and the public network infrastructures.

Gateways for data and voice can include network routers, radio-cum-line hardware switches, multiplexers, and Voice-over-Internet-Protocol (VoIP)-based gateways. Network routers are necessary to perform traffic routing and flow control functions, providing a virtual, packet-carrying end-to-end link from the origin site to the destination site. Routing control between different Autonomous Systems (e.g., Division networks) can be provided by, for example, the Border Gateway Protocol (BGP). Thus, gateways themselves can be interconnected as a network of communications resources.

Data Links

Loosely defined, data links are the means of connecting one system to another for the purpose of transmitting and receiving data.

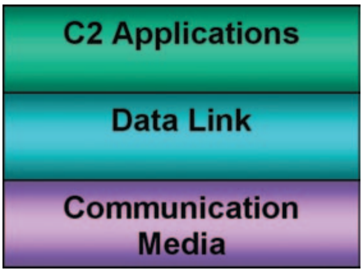

Figure 2: Data link as middleware

A tactical data link is a standardised communications link used for the transmission of digital information and is characterised by standardised message formats and transmission characteristics. Thus, the data link protocols form the middleware between C2 applications and the communications media. See Figure 2.

The SAF ONE Network

When the appliances are connected to the base station in an Access Network, such as a command post, a Local Area Communications (LAC) coverage is formed. Peer-to-peer appliances also provide LAC coverage. The Access Networks and Peer-to-Peer Networks deployed in different areas can be interconnected among themselves or with the homeland Core Network through the Extended Backbone. A Wide Area Communications (WAC) coverage in the battlespace is thus formed, comprising a collection of Peer-to-Peer Networks, Access Networks and the Extended Backbone. The WAC typically spans a large geographical area and provides coverage for a deployed Division.

In this manner, the military battlespace communications infrastructure provides full flexibility and connectivity to where and when they are required. This is the essence of the SAF ONE Network of networks, as shown in Figure 3. Some term this as the military users' Tactical Internet.

In the SAF context, the data link protocol standards are media-independent and thus ride on all the four domains of the Communications Connectivity Model. The SAF ONE Network comprises mainly IP-centric

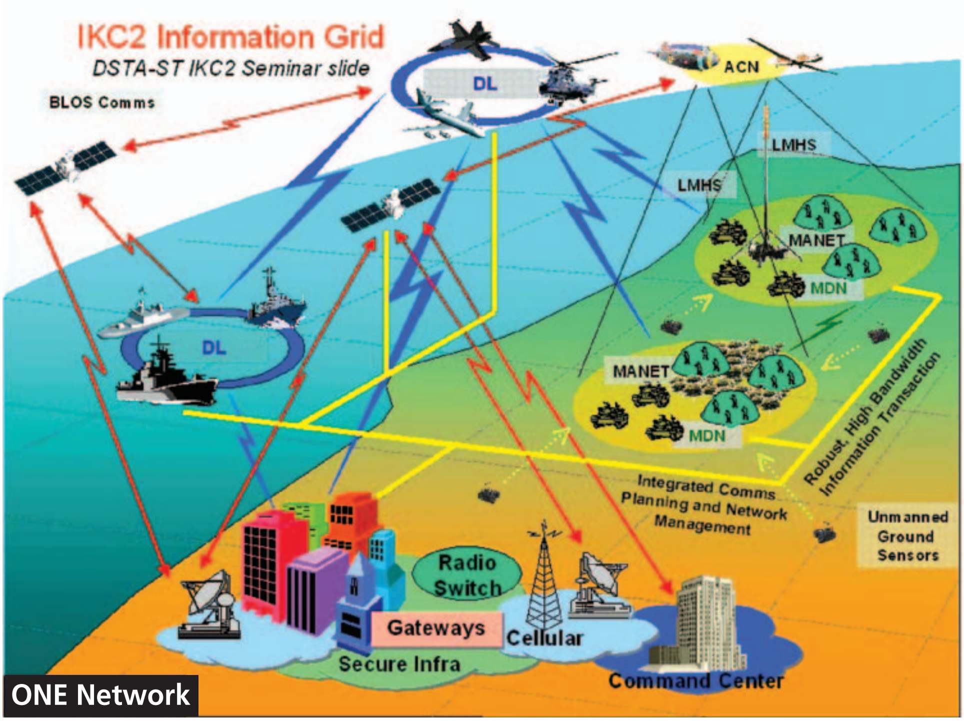

Figure 3: The SAF ONE Network (Source: DSTA-ST IKC2 2003 Forum Proceedings)

networks. Other data links, such as the SAF data links as well as those of the US and proprietary data links, also feature in the ONE Network. Underlying the data links are the communications management services, including network, frequency, quality of service (QoS), security and mobility management (See Figure 4).

Network Management

A unified network management system provides centralised control, monitoring, and execution of network policies with pre-defined user profiles. It provides the commanders in the headquarters with high level visualisation of the health of the theatre-wide network. A comprehensive set of network modelling and simulation tools will enable network planners to model the network accurately and simulate traffic loading. This will help planners formulate network policies on network usage.

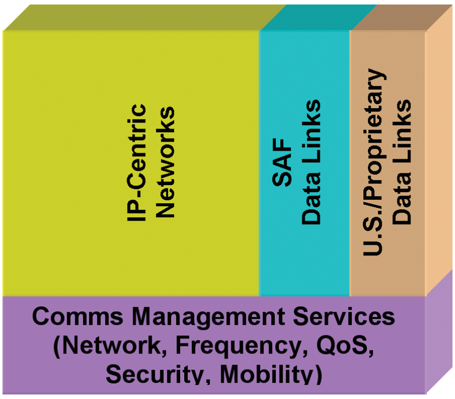
IP-Centric Networks
SAF Data Links
U.S./Proprietary Data Links
Comms Management Services (Network, Frequency, QoS, Security, Mobility)

Figure 4: The ONE Network concept

At the individual network level, decentralised network operations, administration and maintenance systems provide intelligent and real-time control and maintenance of the network traffic. The basic functions are bandwidth provisioning and optimisation in the single network environment. The individual network maintains a knowledge base on the requirements of the command and control systems it supports.

The network management and control functions will evolve, as more effective algorithms emerge. Advanced functionalities such as adaptive routing and more efficient packet switching will change the way networks operate. For example, suitable MANET algorithms allow for multi-node hopping to bridge distant nodes. In the theatre-wide network, traffic will be intelligently routed to the most appropriate system for backbone communications based on extensive network policies (e.g. priority to time-critical information) and user profiles (e.g. priority for commanders), which are to be defined.

Technology Convergence

Communications technologies are evolving and they can overlap in backbone, access or peer-to-peer applications. There are many examples of such convergence.

- WiMAX is designed as an access network using base stations (point to multipoint). However, due to its high bandwidth, it can be used for backbone application especially if directional antennas are used.

- ITT Corporation's Near-Term Digital Radio has a two-tier MANET (which is basically a P2P application) but its radio cluster-heads actually emulate a base station.

- Trunked Radio System (e.g. TETRAPOL) is an access network but its handsets have Direct Mode Operation (DMO) features and can be used as walkie-talkies (i.e. peer-to-peer) without the need for a base station.

- Commercial cellular technologies are dual-use and their cellular waveforms (e.g. TETRA) are planned in Software Defined Radios.

- With the maturity of SATCOM-on-the-move technologies, the mobile satellite ground station can be viewed as having both long haul (extended backbone) and communications-on the-move (access network) capabilities.

THE MODEL AT WORK

Based on the Battlespace Communications Connectivity Model, the envisioned future military communications in the digital battlespace can be synthesised. A complex network can be built by selecting and interconnecting individual communications subsystems. Conversely, any big picture of battlespace communications can be analysed into its component parts by identifying the individual communications subsystems as belonging to the respective domains in the model. See the example in Figure 5.

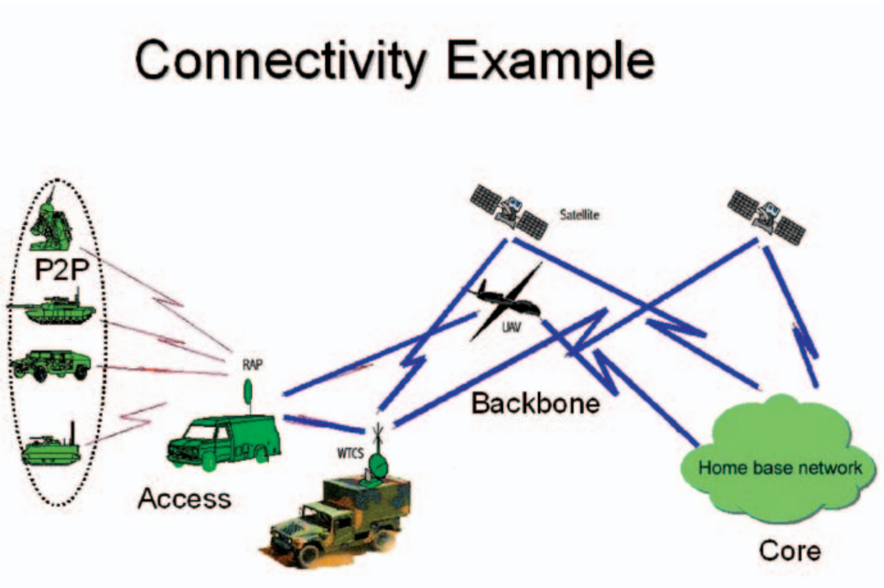

Figure 5: A Communications Connectivity example

UK Military Communications Network

With reference to the Battlespace Communications Connectivity Model, the UK BOWMAN system comes under the P2P network, although it is a two-tiered one. The lower tier is a narrow band capability made up of HF and VHF radios for voice and low data rate communications. The upper tier is made up of High Capacity Data Radios for wideband data communications.

The UK SYNERGY system, which is based on the TETRAPOL PMR cellular system deployed for peace support operations in Iraq, comes under the Access Network. The CORMORANT (high capacity trunk and troposcatter communications), FALCON (tactical level trunk communications) and SKYNET 5 (military SATCOM) systems match the Extended Backbone. Finally, the UK Defence Information Infrastructure corresponds to the Core Network in the homeland.

US Military Communications Network

The US Global Information Grid, which is the communications infrastructure that enables Network-Centric Warfare, can be mapped into the Battlespace Communications Connectivity Model. The Core Network is represented by the Defence Information System Network, which consists of the Non-secure and Secure Internet Protocol Router networks.

The Extended Backbone includes terrestrial systems such as the High Capacity Line of Sight radios, as well as space-based systems such as the Advanced Extremely High Frequency satellite system and the future Transformational Satellite Communications System.

The P2P Network includes radio systems such as the Near Term Digital Radio and Joint Tactical Radio System (JTRS). The Access Network includes adapted commercial technologies such as secured WLAN.

Using the networks mentioned, the Warfighter Information Network-Tactical (WIN-T) programme provides reach-back, interoperability and network operations for all users from the homeland network down to the fighting battalion, and extends to the individual soldier's JTRS software radio systems. WIN-T is expected to support high manoeuvrability of the forces, with full on-the-move, broadband communications capability.

Other notable developments in the US Army include its mandate towards Everything-over-Internet-Protocol to achieve network interoperability, and its work on building a set of data and application standards through common vocabulary and data schema to achieve information interoperability.

CONCLUSION

The Battlespace Communications Connectivity Model serves as an analytical tool for our communications engineers to design feasible solutions and to do trade-off studies while being cognizant of the big picture. Together with a good communications modelling and simulation tool and a process that feeds forward experiences from Operations and Support, it provides the engineers with an objective point of view when proposing the most cost-effective and future-proof solution to meet the operational requirements of the SAF.

REFERENCES

Adcock, Mark. (2002). A Land Tactical Internet Architecture for Battlespace Communications. Land Warfare Conference Brisbane

http://peoc3t.monmouth.army.mil

http://www.globalsecurity.org

Kenyon, Henry S. (2005). Falcon Soars Into Service. SIGNAL Magazine.

BIOGRAPHY

Seah Peng Hwee is Head of Sensing and Connectivity (SENSCONN) Community, which comprises sensors, communications and network professionals in DSTA. He is responsible for competency development and resource management toward organisational capability development. He was previously the Division Manager of the DSTA business unit responsible for all acquisition management of defence communications systems for the SAF and customers. Earlier in his career, he had also worked on radar projects and large-scale Command and Control systems. Peng Hwee holds a Bachelor of Electrical Engineering and Master of Science in Industrial Engineering from the National University of Singapore (NUS). He also obtained a Master of Science in Communications & Signal Processing from Imperial College, London under the Defence Technology Training Award.

Wong Choon Bong is Principal Engineer and Senior Systems Manager (Systems Management). He is responsible for maintaining the health of all Command, Control and Communications systems supporting High Readiness Core operations. A communications engineer by training, Choon Bong has experience in project management and software development in DSTA and system integration for various communications-related projects in the SAF. He has also served as Programme Manager for IT Infrastructure in the Army CIO Office. Choon Bong holds a Bachelor of Electrical Engineering from NUS under the Defence Technology Training Award. He also obtained a Master of Electrical and Computer Engineering from Cornell University, USA, under the DSTA Postgraduate Scholarship.