Ten Ideas for Designing

Next Generation Communications Network

ABSTRACT

The realisation of a robust, integrated and intelligent next generation communications network will form a solid foundation for the Singapore Armed Forces' Integrated Knowledge-based Command and Control. Many challenges remain in our way – a harsh environment, immature science and the limits imposed by the laws of physics. Innovative strategies and cutting-edge technologies are needed to overcome them.

This paper discusses the collective wisdom that emerged from the Communication Architecture and Strategy Forum conducted by the Future Systems Directorate in January 2007. Participants of the forum included representatives from various groups within the defence eco-system as well as external partners. The top ten ideas that were voted by the participants are presented here. Undoubtedly, some of these ideas are difficult to realise but if we can do so, they will benefit us for a long time.

Lee Kok Thong

Ten Ideas for Designing Next Generation Communications Network

INTRODUCTION

The study of network-centric warfare (NCW) has its origins in the 1990s. Network Centric Warfare: Developing and Leveraging Information Superiority, by Stein, Alberts and Garstka, is generally considered by many to be the seminal work in this field. Integrated Knowledge-based Command and Control (IKC2) is the Singapore Armed Forces' (SAF) initiative in taking NCW to the next level – the knowledge edge (Lee, Jacqueline, 2003). IKC2 is one of the key drivers of the Third Generation SAF fighting force. It seeks to organise knowledge and augment battlefield awareness through networking of military systems.

Force is increasingly being realised through information sharing over the communications network. This philosophy places a premium on information superiority on the battlefield and is based on the ability to achieve an Internet-like secure capability in operational areas, providing ubiquitous network access to enable "anytime, anywhere" communications.

CHALLENGES IN COMMUNICATIONS

Building a networked force requires careful consideration of the types of assets that have to be connected. The huge repertoire of entities includes ground troops, armoured and non-armoured vehicles, naval platforms as well as airborne units. In addition, there are command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) assets that may be fixed or mobile. Moreover, the tactical environment is extremely harsh, in sharp contrast to commercial environments.

From marching soldiers to supersonic tactical aircraft, the huge extent of the mobility gap introduces even more challenges (Tong, Swami, 2003) in protocol designs. Undulating terrain and extreme weather conditions further obscure wireless communication. The result can be intermittent connectivity with wide ranging communication delays - from milliseconds to days. The wide operational scenario also presents significant Radio Frequency (RF) propagation and signal characteristics, resulting in poor channel (air or water medium) capacity.

In addition, information assurance presents more stringent considerations. The risk of capture and fear of compromised unattended sensors further limit the usage of sensors. The security elements introduced to the communications system will constitute additional costs to the system.

The introduction of new electronic systems (and consequently more portable power needed) will further add on to the load that soldiers are already carrying. For Special Forces and long-deployed systems, the tactical domain will require even more high energy-efficient solutions. Unlike equipment in the commercial world, military communications equipment have to survive rough handling, heat, dust, sand, salt water, and high humidity. Figure 1 illustrates some of the difficulties that the tactical space imposes on communications technology.

NETWORKING FORUM AND SYSTEMS ENGINEERING APPROACH

In a bid to solicit new paradigms towards the design of next generation wireless tactical communications, the Future Systems Directorate (FSD) organised a technical and strategy forum in early 2007. A wide spectrum of participants - ranging from military users, partners from the local defence ecosystem (DSO National Laboratories, DSTA and ST Engineering) to research academics (I2R) and external participants (Cisco Systems and General Dynamics Canada) – was invited. This was an inclusive effort to bring all key stakeholders together to discuss and debate about new concepts.

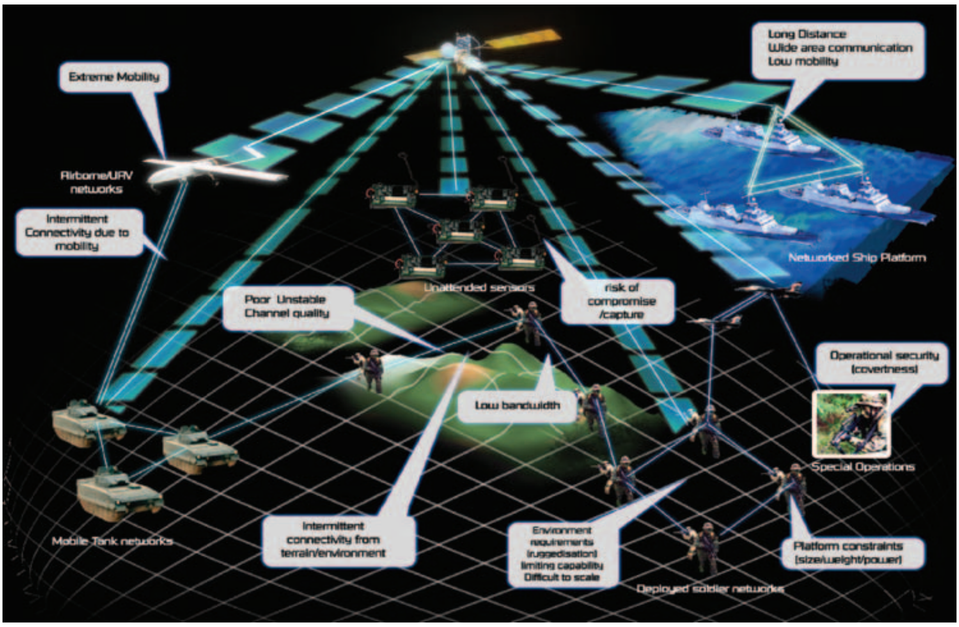

Figure 1. Challenges faced in a wireless tactical environment (Burbank et al, 2006)

Many ideas were mooted and there was a generous exchange of views during the forum. Many of these ideas raised remain hard to realise. They can be described as "FSD-hard"[1] kind of problems. However, the payoffs are big even if we are able to unlock just a few among them. Some of them might emerge as breakthrough ideas that will go a long way for us.

The participants voted for the 10 most promising ideas at the end of the forum. The following is a discussion of these top 10 takeaways.

TOP 10 IDEAS

Idea#1: Adapt Cross-Layering Against Stove-pipe Open Systems Interconnection Layers

The fundamental protocol building block for the Internet is the Transmission Control Protocol/Internet Protocol (TCP/IP). Originally conceived for the wired Local Area Networks, TCP/IP was re-used when protocols for the wireless network were needed. Experiments have shown that the transmission of video over current wireless media (such as WIFI) is riddled with unsatisfactory experiences such as video "freeze" and jerky images.

To start with, the TCP/IP protocol designers did not take into account that the wireless transmission medium is impaired by negative effects such as fading and co-channel interference. Moreover, the bandwidth of the radio-frequency transmission is limited and power is usually too scarce to satisfy the demands of video. The advancement of computing and programming tools has made applications even richer. Today's wireless network will need to carry different types of traffic - voice, video and data, each having its own characteristics.

Furthermore, we have to re-examine the fundamental way protocols were designed in the Open Systems Interconnection (OSI) Model. The OSI layer consists of seven layers, as seen in Figure 2. Data going to and from the network is passed from layer to layer. This way, each layer is written as a modular software component. From the software design point of view, it is efficient but as a system, the independent design of different layers may yield a grossly sub-optimal network.

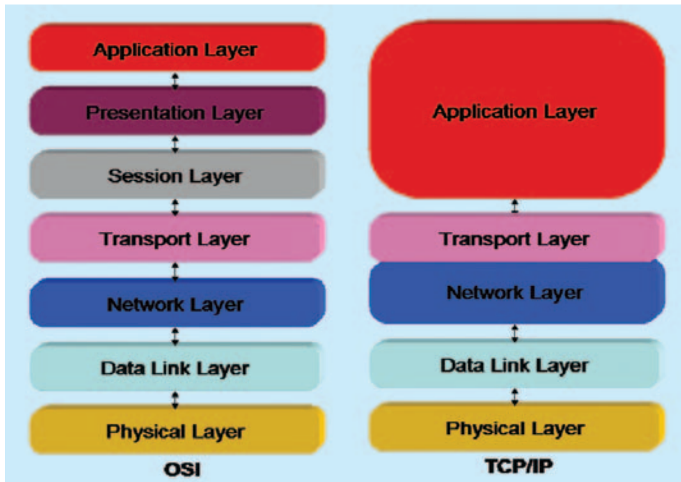

Figure 2. OSI and TCP/IP

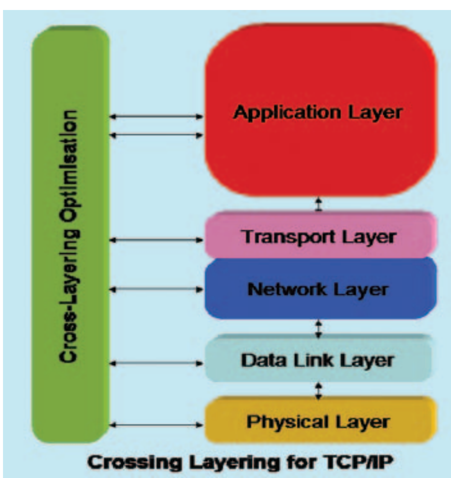

Figure 3. Cross layering optimisation

To break out of these limitations, the new goal for communication designers is to analyse a cross-layer (Lin, Shroff, Srikant, 2006) that will yield jointly optimal physical, medium access and routing layers for wireless networks. Cross-layering will allow for sharing and better understanding of different layer performance to make system-level decisions. Figure 3 depicts how cross-layering architecture can occur in the TCP/IP architecture. Currently, cross-layering architecture is a hotly researched topic which has already begun to show some promising results (Nahm, Helmy, 2005).

Inevitably, as a new design paradigm, cross-layering architecture will raise other issues: which and how many layers should be integrated? How do we manage cross-layer overheads and parameters exchange and consequently the delay to end-to-end applications?

In the course of FSD experiments, an innovative and successful start-up company VSEE was discovered. VSEE exploits cross-layering techniques to enhance video conferencing experiences over the Internet. VSEE reserves a dynamic and small portion of the network bandwidth to do video conferencing; it does so by constantly monitoring the amount of instance capacity available at the physical channel and adaptively adjusts the video stream using its proprietary compression technique. VSEE was able to maintain a good video quality despite the low-bandwidth of no more than a few 100Kbps .

Idea#2: Tailored Solution to Specific Ops Context

The concept of mobile ad hoc networks (MANET) is not alien to military users today. A MANET network consists of a collection of mobile nodes communicating in a multi-hop

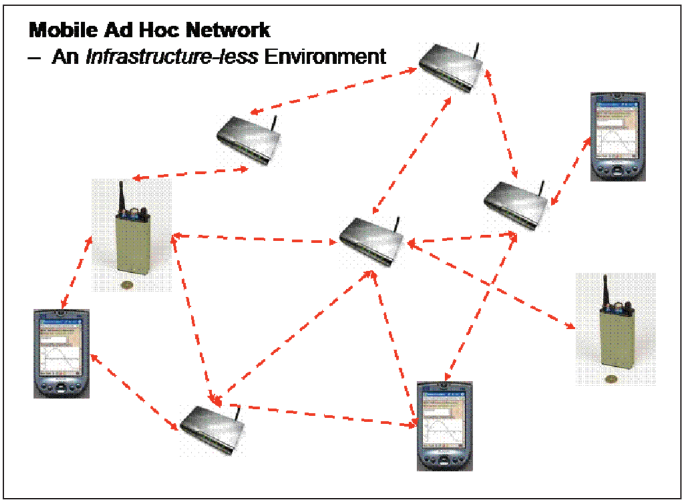

Figure 4. Mobile ad hoc network

way without any fixed infrastructure such as access points or base stations. This is particularly useful in military applications or disaster recovery operations.

Commercial interest in such networks has been growing steadily. However, conflicting needs in designing MANET parameters such as routing, security, Quality of Service (QoS) and power consumption often mean that compromises have to be made. As a result, any direct adoption of commercial MANET solutions is often met with unsatisfactory outcomes especially in the military operational environment. Experiments have further indicated that commercial MANET solutions are still a long way from maturing into deployable solutions that can scale and work well under more stringent operational context. Customisation of Commercially-off-the-Shelf (COTS) MANET products to the specific operational context in which they will be deployed is therefore needed.

As an example, consider the choice of routing protocols which are critical to MANET scalability. Two broad types exist: proactive or reactive ones. Proactive routing protocols actively broadcast to achieve a converged network at the expense of more controlled traffic while reactive routing protocols passively wait for new nodes to identify themselves, hence reducing the controlled traffic albeit with slower convergence. Many research efforts have been poured into deciding the "winner". Nonetheless, a single optimal solution does not exist for all military contexts.

To build a practical, operational MANET solution is to tailor specific solutions according to the relevant operational context.

Idea#3: Put Commercially-off-the-Shelf Strategy at the Core

Metcalfe's law states that the power (value) of a telecommunications network is proportional to the square of the number of users of the system (n2). The value grows non-linearly with the number of nodes in the system. Likewise for IKC2, the power of the communications network grows with the proliferation of tactical radios all the way to the "last mile" i.e. the lowest fighting echleon. Traditional Very High Frequency (VHF) / Ultra High Frequency (UHF) / High Frequency (HF) military radios have limited capacity. Consequently, the commander's situation awareness is largely impaired. The development and advancement of tactical radios have been slow, hampered by the lack of demand due to the small market. Military tactical radios remain expensive, making proliferation to the lowest echelon difficult. See Figure 5 for cost development trends. In contrast, cost reduction for commercial radio is often fuelled by civilian needs, which far outweigh that of the military.

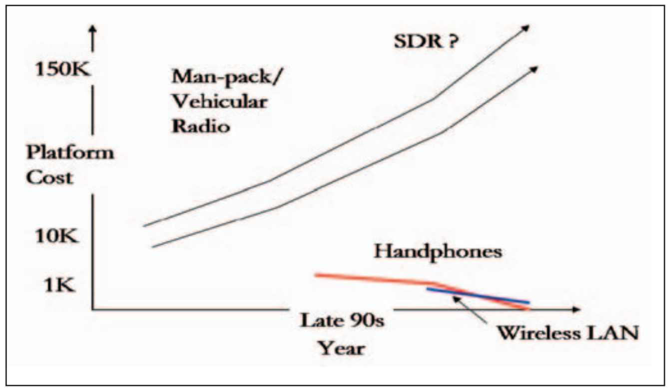

Figure 5. Platform cost over time

COTS Wireless LAN such as WIFI is several orders cheaper yet provides several orders more bandwidth than any of the digital tactical data radios available. Even before WIFI was adapted, IEEE had already ratified a newer and better standard, WiMAX, in 2006, which offered up to seven times more bandwidth than WIFI per client and other advanced features such as security and QoS. There are many more breakthroughs coming from the commercial sector as the amount of research funds and effort is tremendous. COTS communication solutions put more pressure on military vendors. We should find means to exploit these exploding trends. They will assist us to realise true affordability and massive proliferation. "Put COTS at the core" represents a gigantic step in the changing of mindset towards military acquisition strategy.

Idea#4: Identify Correct Requirements through Iterative Process and Ops-Tech Integration

Besides playing its traditional roles, today's SAF is also called upon to perform other tasks such as humanitarian and relief efforts. This exacerbates the difficulty of military planners in predicting the needs of future operations. The difficulty is often due to the unpredictable nature of conflict and the inadequacy of information at one's disposal.

The BOWMAN project is a case in point. BOWMAN is the UK Armed Forces' multi-billion battlefield digitalisation programme. The programme, which commenced in the late 1980s, was due for full system delivery in 2007. In the 2006-7 report, the UK Public Accounts Committee (Page, 2007) reported that BOWMAN suffered from several lapses and serious delays in delivering the system. One of the reasons cited was the lack of proper initial project understanding between the programme's technical side and the Ops users.

The SAF believes that technology is a force-multiplier. Investing correctly in core technologies will be critical to the SAF. DSTA is poised to identify and manage technology. This helps the SAF to better respond to the "gaps" caused sometimes by poorly defined or unexpected requirements. A tight and equal Ops-Tech integration partnership, coupled with iterative rounds of open examination, is therefore key to identifying the right requirements for future communication needs.

Idea#5: Use Systems Engineering Solution to Solve Complex Problems

Building an IKC2 communications network to support the Third Generation SAF is a complex task. Interoperability with legacy systems and striking a balance between the Services' divergent needs are just some teething issues that need to be overcome. For example, navy ships move significantly slower than airplanes and are more widely spread out than army troops. Employing a systems engineering approach is therefore akin to identifying the

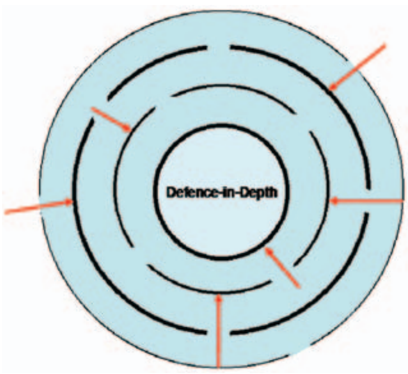

Figure 6. Defence-In-Depth multi-layer defence concept

right ingredients that will make up the future communications solution.

Consider the problem of jamming to tactical radios at the command post; one non-systems approach would be to consider more power or sophisticated anti-jamming algorithms. The outcome is a more expensive radio without any real capability improvement. An expanded approach is to include possibilities derived from systems analysis such as non-related domains or even non-technical solutions. In this case, a non-RF solution such as using Free Space Optics (FSO) can be cheaply implemented for inter-command post connectivity. FSO is frequency-jam free and more secure due to its limited narrow beam.

Another useful concept is defence-in-depth. It is the practice of layering defence to provide a robust, comprehensive, systems-level protection against attacks and intrusion attempts. Each defence strategy may not be comprehensive and is probably effective against only specific attacks (and therefore cheaper to implement). Collectively, they are very powerful. The defence-in-depth strategy slows down the attack while allowing the system to recover and perform counter measures. People, technologies and operations are three main areas that the defence-in-depth strategy could use to provide a robust protection architecture for any IKC2 network.

Idea#6: Overcome Trade-offs by Working in Alternative Space and Adaptive Radio Software

"An ideal wireless communications system would provide high data rates at very long range and yet use minimum power and bandwidth. Such a system would overcome problems and perform well despite the challenges of channel weakness such as signal fading and interference. Adding on to these features, the cost of fabricating such a communications system with transmitters and receivers would be kept at a minimum and affordable for mass proliferation."

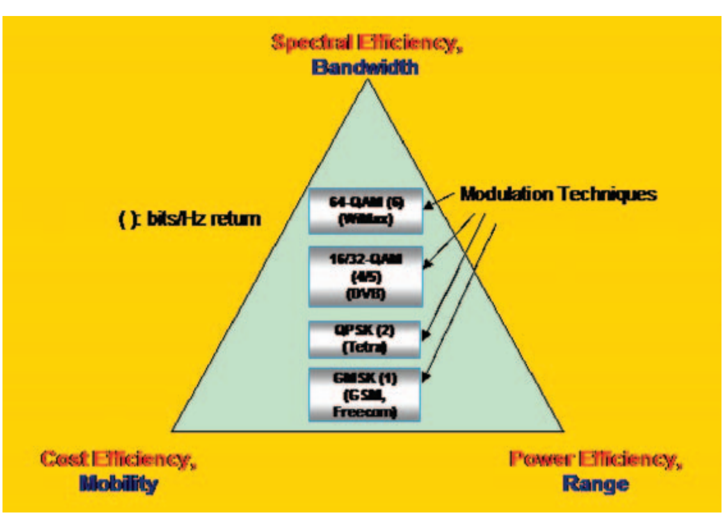

Figure 7. Trade-offs – "triangular" relationships

This is a description of a system that has yet to be built because multiple and mutually exclusive objectives such as low cost, small size, high reliability, and large capacity make it difficult to do so. The systems architect would need to study the trade-offs among different combinations of modulation, coding, multiple access, and antenna techniques to determine the best design. Figure 7 illustrates some of these fundamental "triangular" trade-off relationships - "spectral efficiency, cost and power" or "Range, mobility and bandwidth"[2].

How can we achieve breakthroughs despite these constraints? The basic assumption on the usage of military radio is that most researchers have tried to solve the power-range trade-off on the ground. Radio propagation on the ground does not travel far as it encounters obstacles like foliage and urban static features. The signal's penetration is low and its quick attenuation with distance reduces the communication range. With the advancement of microcomputers and unmanned air vehicles (UAVs), the cost of providing an airborne communications service over a broad area can be drastically reduced. It is akin to a mobile GSM base station mounted on a UAV. In fact, such a strategy completely transforms the "triangular" relationship.

The fabrication of traditional radios is fixed once the radio engineer has selected a fixed solution (triplet) on the "triangle". Fixing the radio solution limits the context in which the radio can be used. Software-defined radios (SDR) and cognitive radio (CR) concepts seek to break out of this restrictive approach. The SDR concept reduces radio cost by re-using the same radio chassis for different waveforms adapted for different scenarios. The waveforms are digitally inserted into the radio and can be re-loaded at any time. Cognitive radio is another paradigm for wireless communication in which wireless nodes adaptively change their transmission or reception parameters to communicate efficiently without interfering with licensed or unlicensed users. CR adapts and increases communication capacity according to the feedback received.

Idea#7: Use Spiral Development Against Fast Obsolescence

Newer variants of radio are coming out at a faster rate due to COTS advancement, notably in electronics. Many military programmes can become hostages to the speed of advancement in commercial standards and demands. Moreover, the existing quantity of the radios in the military inventory means that the military cannot afford to replace them overnight. Such a strategy presents a high risk in that a wrong bet would result in an instant write-off of hundreds of millions of dollars. Moreover, massive re-hauling of one's radio capability is often a long and tedious process.

The global war on terror as well as Operation Iraqi Freedom has prompted the US Department of Defense to expedite the delivery of the latest weapons systems and protective equipment to the troops deployed at the frontline[3]. Rather than developing, testing, and then fine-tuning systems before sending them to the field, the priority is to get new technologies to the troops as quickly as possible, while continuing to improve on them in the laboratories. Such is the essence of the spiral development approach.

Spiral development offers mitigation against technological obsolescence. It does so by continually allowing the insertion of technology into long-term projects. Coupled with the strategy of COTS exploitation, this presents a powerful acquisition approach.

Idea#8: Standardise Only at the Lowest Denomination

The navy, air force and army conduct their operations in vastly different tactical environments. To fully equip the army, it would require a large number of communication devices whereas to fully equip the navy and the air force, it would require significantly less effort. Fighter aircraft and UAVs are high-speed platforms whereas ships and convoys move much slower on the ground. The infantry has to navigate through vegetation and undulating terrain whereas aircraft have to grapple with cloud and airspace coordination. Underwater communications is altogether another domain of expertise as acoustic waves trump electromagnetic ones. In short, each Service has its own specific requirements used in the design of their optimal communications radio.

However, the realisation of a networked force means that some form of interconnectivity and interoperability among the services is needed. This will likely require some form of standardisation. Yet standardisation has the pitfall of satisfying the common needs but failing to deliver optimal solutions specific to each individual Service. Where should we draw the line?

As the Third Generation SAF grows, it will get more connected and complicated in the process, while inter-Service traffic profile will gain more importance and the conventional "80-20" wisdom will apply less. A more suitable response would be to adopt the policy of "standardisation only as a last resort". More specifically we ought to standardise designs at the ***lowest common denominator*** applicable.

The Internet was designed on the principle of standardisation at the lowest common denominator. The usage of TCP/IP provided baseline stability. It is anticipated that open, voluntary standards and flexible communication protocols, such as IP, will play a key role in fulfilling the goal of designing multimedia-rich information exchange applications and services based on mechanisms and frameworks that are hidden from the users.

Idea#9: Delay-Tolerant Networking Against Extreme Network Conditions

The assumption made by Internet designers for TCP/IP is that the end-to-end round trip time of the data is short; no more than a few seconds. This is valid as devices within the Internet are generally connected via hard physical wires, which makes transmission quality quite reliable. Otherwise, the circuit will be dropped. Hence it would be catastrophic for NASA to design a communications protocol using TCP/IP for communication between Earth base stations and probing devices for Mars.

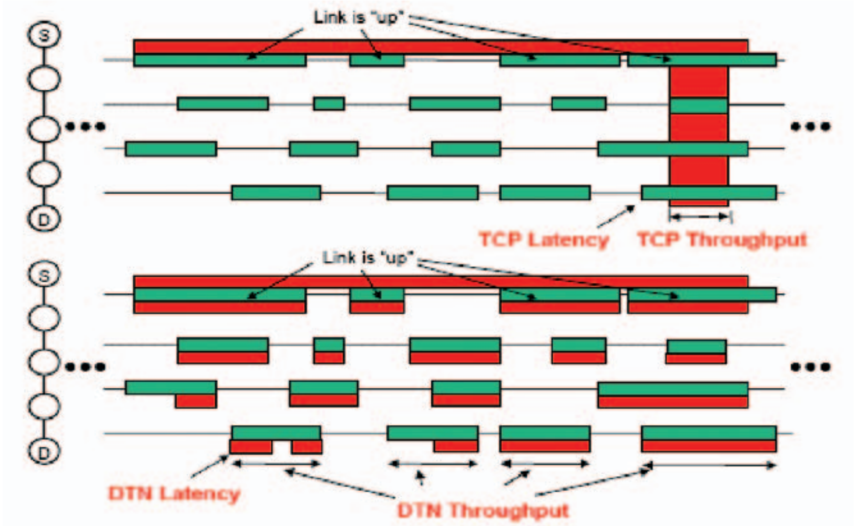

Figure 8. Delay Tolerant Networking, (Source: ATO, DARPA)

Harsh operational environments characterised by non line of sight, high terrain and high mobility makes no guarantee of end-to-end connectivity. This results in unreliable networks and high link error rates. Moreover, intermittent links are sometimes required to save power. It is also caused by scheduled transfers of unattended devices, so as to limit congestion. A military communications network consists of a number of independent networks, each supporting specialised communication requirements. These networks do not necessarily use IP and they are often mutually incompatible in that each is good at passing data within the network but is not able to exchange data among one another.

Delay-Tolerant Networking (DTN) (Warthman, 2003) or Opportunistic Routing is the study of new innovative techniques to help communications engineers design better network appliances to fight these challenges. DTN is an overlay on top of the heterogeneous "regional" networks. It supports interoperability of these "regional" networks by accommodating long delays between regional networks and within each network via the translation of regional network communication characteristics. DTNs overcome the problems associated with intermittent connectivity, long delays, and high error rates by using store-and-forward message switching, caching of in-transit data packets, message ferrying and connection state hibernation for subsequent reactivation. Studies conducted by Intel and Berkeley (Demmer, 2004) have indicated a significant improvement when DTN techniques are employed. In some cases, DTN produces throughput that is close to the theoretical maximum throughput achievable.

Idea#10: Manage Mobile Bandwidth as a Scarce Resource: Policy-based Quality of Service

Bandwidth is a scarce resource that has to be managed carefully as more applications such as video streaming, which make intensive use of bandwidth, become commonplace.

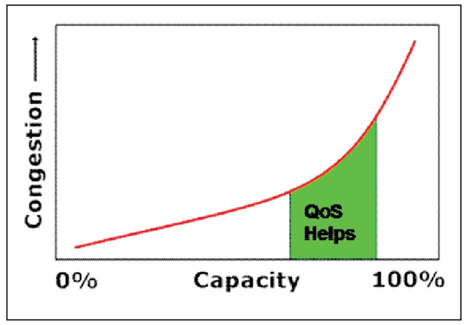

Figure 9. Where QoS matters

QoS refers to "control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application programme." QoS guarantees are important especially if network capacity is limited, as seen in Figure 9.

The current generation of Internet is still "best-effort". QoS will be particularly important in the military context. Data in military networks comes in various forms, ranging from chats, emails to command and control data and intelligence reports. Building separate networks for each of these applications runs against the spirit of a networked force. Data differentiation or prioritisation will make our network more responsive and intelligent, especially in situations where data traverse non-homogeneous environments.

There are however considerable challenges in implementing practical QoS due to the high and unpredictable mobility of troop forces and aerial platforms. Enabling QoS in tactical communication environments requires some form of "network stability". QoS degrades quickly as the mobility of end nodes increases. In turn, re-transmission of dropped data leads to a worsening of the traffic congestion. One idea for ensuring QoS in ad hoc mobile environments is to build a core set of wireless nodes that are relatively static - controlled mobility nodes - in order to provide a baseline support backbone. Implementing QoS policies within this backbone is then achievable and allows the system to maintain a high standard of service.

Policy-based QoS refers to the middleware services that decision-makers such as commanders can use to interface directly with their network resources, such that they can assign and control these resources while understanding the implications of their actions. Policy-based QoS can be made on the fly and quickly disseminated to all system nodes. This ensures that the underlying network resources do not operate in a black box.

Routers located at the edge of the network are the first recipients of data from the end user devices. They simply accept and relay the data to its designation. Even when the network is congested, edge routers continue to inject data indiscriminately into the system. This can result in sudden network outage. Network admission conditions and traffic shaping tools (Bidgoli, 2007) are powerful techniques that can help to manage congestion. Data that do not fulfil criteria ought to be prevented from entering. Policy-based schemes could implement the supportability of certain data/video formats. The result will be an intelligent network capable of recovery from congestion.

CONCLUSION

We have presented the top 10 strategies for designing next generation tactical communications networks, based on the collective wisdom of diverse stakeholders.

We recognise that many hard challenges still need to be overcome before the ideas can be realised. Some of the suggested technologies are still in their infancy while others are more ready to be adopted. These are very tough issues, and once we are able to overcome some of them, they will emerge as potential disruptive breakthroughs for us.

These strategies are by no means exhaustive. However, together they represent a formidable plan to move ahead as we seek to design and build a robust, intelligent and dynamic IKC2 network for the Third Generation SAF.

END NOTES

1. Note: Borrowing a phase which current Director of US DARPA, Dr Tony Tether likes to say, "DARPA-hard" questions, which means problems that are so hard to overcome that only DARPA will contemplate.

2. Henry Lee et al. Connectivity for Network Centric Warfare is still a Far-Fetch Dream?, Cutting Edge Communication Architecture Forum, 2007. Employing a highly spectral efficient modulation technique such as 64-QAM means that for every bandwidth (measured in Hz) used, we are able to derive more data (in terms of bits). However this often means that sacrifices have to be made on cost efficiency (more expensive and less stable electronics) as well as power efficiency (a higher signal-to-noise figure is thus needed and this translates to high receiver sensitivity, often harder to achieve.)

Note: In 2005 and 2006, the Aberdeen Test Center's scientists, technicians and engineers tested about 30 rapid fielding initiatives a week, with more than 1,400 tests conducted in 2006 alone. There has been an 87 percent increase in range activity here since fiscal 2001. Source: http://www.technologynewsdaily.com/node/6336

REFERENCES

Bidgoli. (2007), The Handbook of Computer Networks, Network Traffic Management. Wiley.

Burbank, Chimento, et al. (2006). Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. The Johns Hopkins University Applied Physics Laboratory, IEEE Communication Magazine.

Forrest Warthman. (2003). Delay Tolerant Networking: A Tutorial. Retrieved on Sep 2007 from http://www.ipnsig.org/reports/DTN_Tutorial11.pdf

Lee, Jacqueline et al. (2003). Realising Integrated Knowledge-Based Command and Control, Transforming the SAF. Pointer Monograph, Singapore Armed Forces.

Lin, Shroff and Srikant. (2006). A Tutorial on Cross-Layer Optimization in Wireless Networks. IEEE Journal on Selected Areas in Communications on ``Non-Linear Optimization of Communication Systems'', vol. 24, Issue 8, [pp].

Michael Demmer, Eric Brewer, Kevin Fall, Sushant Jain, Melissa Ho, Rabin Patra. (2004). Implementing Delay Tolerant Networking. Intel Research Berkeley.

Nahm, Helmy et al. (2005). TCP over Multihop 802.11 Networks: Issues and Performance Enhancement, MobiHoc.

Page, Lewis. (2007). MPs: UK defence project was crap. Retrieved on 1 Oct 2007 from http://www.theregister.co.uk/2007/03/08/bowman_cpac_pasting/.

Ripley, Tim (2007), Bowman misses the target. Retrieved on 15 Sep 2007 from http://www.global-defence.com/2001/CSpart1.html.

Tong, Swami et al. (2003). Future Challenges of Signal Processing and Communications in Wireless Networks. NSF/ONR/ARL Workshop.

BIOGRAPHY

Lee Kok Thong is Principal Engineer (Systems Architecting) and was Assistant Director (Future Systems Directorate). In that capacity, Kok Thong helped the Future Systems Architect formulate alternative concepts that were not in the mainstream, conducted experiments for the validation of new concepts through exploiting technology, performed the role of institutional red-teaming and oversaw the collaboration in experiments with external partners. He graduated with a Master of Science in Telecommunications from King's College, London and Diplome D'ingenieur (French), Fondation EPF in 1998 under the Overseas Government PSC Scholarship. He obtained a Master of Science in Defence Technology and Systems from National University of Singapore and Master of Science in Computer Science from Naval Postgraduate School in 2004. He won the Defence Technology Prize (Team) in 2002, as well as the DSTA Team Excellent Award in 2002, 2003 and 2006.