Stuart Marsden, PhD-student in Military Technology, National Defence University, Helsinki, Finland, Dept. of Military Technology, stuartmarsden@finmars.co.uk

Jouko Vankka, professor of Military Technology, National Defence University, Helsinki, Finland, Dept. of Military Technology, jouko.vankka@mil.fi

PROVIDING A TACTICAL DOMAIN FOR AN INDEPENDENT NATIONS TASK FORCE

Key words

C4I; tactical; communications; acquisition

Abstract

Any independent sovereign nation will wish to ensure that their land forces are equipped to protect that nations interests. Technology for Command, Control, Communications, Computers, & Intelligence (C4I) systems is advancing rapidly and even smaller nations must keep up. This paper looks at the types of considerations when planning and equipping a task force from the soldier platform to the upper tactical echelon. The paper will consider some of the key technology enablers that can deliver operational benefit. An acquisition approach will be proposed to ensure freedom, flexibility and value for money. Interoperability and other not material development areas will be considered.

Introduction

As we look towards future military equipment and ways of working there are many aspects that must be considered. Technology drives much of the advancements but does not by itself deliver the operational benefits and capabilities that are required. It is important to consider all the development lines used in the US Joint Capabilities Integration and Development System (JCIDS, 2012): Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTmLPF-P). Whilst this paper concentrates on the Materiel or Technology any architecture and system must be implemented in a framework that delivers a complete system.

The topic has been approached in the context of an independent tactical force and starts from the soldier/platform level to the upper tactical echelon. As an example this would be a Brigade size force with armoured, mounted and dismounted elements. This would include organic artillery, engineer, signals and logistic support. In addition they would have attached air and naval assets and a Special Forces (SF) component.

The Area of Operations is considered to be in the defence of the home nation. However, flexibility is retained as a key requirement and no assumption is made about fixed communications infrastructure. The proposed technologies are therefore applicable for more expeditionary operations.

The time frame for the new capability is 2035. The various technologies will however mature at different rates and could be ready much earlier for insertion in to a legacy system. This will be covered later when considering a transition plan.

Whatever the time frame some limitations will remain. Size Weight and Power (SWaP) requirements especially for the dismounted soldier are going to cause constraints. Access to the electromagnetic spectrum will remain finite and contested by other users and the enemy. Some of the technologies assessed may work more efficiently within these constraints.

This paper assesses some of the technology areas in the first two sections divided in to communications and the application layer / software infrastructure. In the next section an architectural approach is proposed with examples in the following section. The paper then puts the system issues in context of other lines of development before concluding and suggesting future work.

Communications

Networks with the ability to pass data and voice are already common in the military domain. However, at the lowest tactical level the access to high throughput data which is connected to a larger tactical internet is not ubiquitous. New equipment such as Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) and biometrics demand a data rate that is not currently available. Some technologies which can help to close this gap are:

Software Defined Radio (SDR). In the same way that a general purpose computer can run different software applications, a SDR can be reprogrammed to have different waveforms and frequencies.

Mobile Ad-hoc Networks (MANET). These networks are able to form networks and allow data to travel between each radio and 'hop' across multiple radios.

Cognitive Radios. These radios are more intelligent in their use of the electromagnetic spectrum. They can detect where a clear channel is available and use it possibly multiplexing many different channels to increase throughput.

Software Defined Networks (SDN). Enabling the inter connectivity of heterogeneous networks is a skilled job which often requires proprietary knowledge of different network equipment. SDN address these problems by allowing dynamic and standardised ability to monitor and configure networks.

Software Defined Voice Networks (SDVN). All informed voice remains the most common method of command and control in dismounted forces. SDVN allow voice to run on top of data and thus voice networks can be defined dynamically.

Software Defined Radio

SDR has the potential to make the selection, upgrade and operation of military radios more flexible. In the same way that a Personal Computer (PC) allows the selection and use of software to suit an operation, a SDR could allow flexibility (Mitola, 1995). The Software Communications Architecture (SCA) was born out of the Joint Tactical Radio System programme and provides a standard framework to describe radio waveforms (Bard and Kovarik, 2007). For an independent nation the benefits of SDR could be marginal, as using an SDR to run only one set waveform delivers no benefit. For a coalition the ability to share a waveform and communicating directly can be desirable for latency and ease of interoperability. The security considerations however may preclude such a direct connection. An SDR could have the benefit of allowing a suite of waveforms to be selected depending on the frequency or the type of communication (satellite, terrestrial or ground to air) (Vankka, 2005). A non SDR also gives this possibility but does not allow a waveform to be added after the radio has been purchased.

The waveforms in the military space remain proprietary and vendor-specific. It is possible that by 2035 they will have become more commoditised and generally available in the same way that cellular standards are published openly. At this point SDR has not delivered the hoped for benefits and programs such as JTRS have had limited success (Goeller & Tate, 2014). SDR could allow the addition of active Combat Identification to a more standard waveform. The radio could monitor an interrogation frequency at set time frames and respond when targeted by Air or other assets.

MANET

MANET allow networks to be formed at the lower tactical level without detailed engineering. They use different approaches to sharing routing information but with the same goal of allowing data packets to be passed across the network (Royer. & Chai-Keong, 1999). Whilst MANET can impose its own issues on security, military variants have link encryption and added transmission security (Singh, Joshi & Singhal, 2013). MANET are already in service today but are restricted to the platform level. Soldier worn MANET data radios are just starting to appear but have limitations on range and must be incorporated to the wider tactical architecture to be fully usable. This is non-trivial for fully dis-mounted operations due to the need for a soldier-worn bridging node to a data backhaul. In mounted operations this is easier to achieve as the equipment can be carried and powered by the platform. This could lead to the requirement for a 'mother-ship' even in dismounted operations. This platform could be an autonomous robot or even an Unmanned Ariel Vehicle (UAV) which would have the added benefit of range and possible ISTAR functions.

Cognitive Radio

The lack of available spectrum is and will remain a key restriction in military communications. The current method of allocating chunks of spectrum is inflexible and inefficient (Akyildiz, et al., 2008). A more intelligent and dynamic way of using the spectrum could be enabled by cognitive radio (Mitola, Maguire, 1999). This would maximise access to available spectrum and thus throughput whilst also simplifying battlespace spectrum management. There are no current true cognitive military radios but many MANET display similar properties, as a side effect of how they are implemented. Cognitive radios are being actively developed but the main barrier is procedural as spectrum managers need to progress from allocating chunks of spectrum for set times.

Software Defined Networks

As more complex and capable data networks begin to move in to the lower tactical echelons support becomes a problem. Signals trained soldiers with the required skills are not available at these levels and however, the soldiers have to concentrate on their primary role. MANETs go some way to abstracting complexity by forming mesh networks autonomously. However different equipments will tend to be linked by routers and need some element of configuration. This will be done prior to the commencement of operations but may have to be changed to reflect changing priorities. There needs to be a way to make these changes remotely and simply. SDN technology has the ability to do this and OpenFlow has become the open standard to implement (McKeown et al., 2008). It will allow remote monitoring/management and should be consistent across different equipment types. Current military communications systems have management software but it is often coupled to the manufacturer or system integrator. Insisting on SDN standards for network management can remove this restriction. The flexibility of OpenFlow can come at the cost of processing overhead and additional latency (Jarschel et al., 2011). Military networks do tend to have much more significant throughput and latency restrictions than OpenFlow may introduce and thus the flexibility becomes the key factor.

Software Defined Voice Networks

The use of all informed voice is integral to the command and control of tactical operations. Historically this has meant a dedicated radio (e.g HF, VHF, UHF) with a common frequency and, more recently, a shared cryptographic key for secure voice. In order to establish new voice network the radio and security key must be shared with the radio. Sometimes this can be done over the air but is often is often restricted by security requirements. This means having to physically move to each radio causing delays and risking lives. Generally one radio means one voice network and thus command vehicles requiring multiple radios and antennas.

As data communications become ubiquitous at the lower tactical levels another approach could address these concerns. Software Defined Voice Networks (SDVN) could allow voice networks to be abstracted on top of data. This is common place in telephony by the use of Voice over IP (VoIP) protocols (Ha & Yang, 2013). These underlying technologies can also be expanded to cover all informed voice. In the tactical domain the use of servers provides single points of failure due to enemy action, equipment failure or RF propagation. Therefore SDVNs need to be fault tolerant and distributed.

Commercial Off The Shelf

The military does not lead the way in communications any more with the mobile revolution having greatly advanced the state of the art (Hartman, Beacken, Bishop, Kelly, 2011). Military systems can save money and adapt more quickly by making use of Commercial Off The Shelf (COTS) technology. In communications the latest 4G standards offer large data rates, mobility and compatibility (Bhattacharyya & Bhattacharya, 2013). By 2035 this will have advanced further. A flexible military system will leverage these technologies but must be aware of the limitations. They were designed for the civil markets and do not have the same requirements as the military. For best utility a cellular system requires a dense network of base stations each with their own backhaul to the larger network. This is not available for early entry warfare but could possibly be established for defence of the home base or utilise the civilian infrastructure. In this case these key communications nodes would be vulnerable to attack by adversaries both kinetically and by cyber attack. The 4G standard does not have the same standard of security that is expected in military systems (Clancy, Norton, Lichtman, 2013). Whilst the security of the data can be layered on top of the network it is harder to add Communications Security (ComSec). These networks are thus vulnerable to spoofing and denial of service attacks.

COTS communications have established bands which are allocated throughout the world. These bands tend to be fully allocated and cannot be assumed to be available to the military in anything short of general war. In coalition operations there could also be multiple users trying to leverage the same technologies and frequency bands.

These limitations on the use of COTS technology can be mitigated with a number of approaches. The COTS technology can be militarised. The waveforms can be used adding additional ComSec. They could also be rebanded to more available military bands. Doing this adds to the cost and loses some flexibility but can get some of the benefits and remain more economical than technology developed purely for military use.

Cell based technology can be more widely utilised with the adoption of femtocell base stations. These can be fitted on platforms or part of the 'mothership' concept mentioned earlier. This would provide a local cell service usable by dismounts with standard smartphone type handsets. The range will be greatly reduced from a planned fixed base stations but depending on the type of warfare and terrain could cover a platoon or company size group. The femtocell will have to have its own MANET to connect in to a wider network. In more difficult terrain satellite connections could be used.

Application Layer and Software Infrastructure

The provided communications network gives the ability to share information between the required software applications. This will include Battle Management, Messaging, Chat, ISTAR and other special-to-arms applications. Whilst we can predict some of these applications, each different operation and task will have its own Information Exchange Requirements (IER). This in turn will lead to different requirements and potentially new software applications. Coalitions also may require the use of new applications. The way that these applications communicate with each other is through protocols and data formats. Whilst standards do exist there can be many competing ones to choose from and they can be inconsistently implemented. Some key areas of software, protocols and formats that driving the design of the tactical architecture will be considered in this section.

Protocols

Applications communicate using protocols. There are several levels that these operate starting at the physical layer or Layer 1/2 in the OSI model (Zimmermann, 1980) which includes Ethernet and Wi-Fi up to the application layer (Layer 7). Adopting these standards makes communicating easier. At layer 4 we have Transport Control Protocol (TCP) and User Datagram Protocol (UDP). These protocols are at the heart of the modern network and universally supported. Most military data radios support TCP and UDP, however the choice of which can greatly affect the efficiency of the network.

TCP is a connection oriented protocol and positively establishes a connection before any data is sent (RFC792, 1981). TCP suffers from a number of well-known performance problems, which become more severe with longer delay, frequent errors, and large bandwidth (Vankka, 2013). UDP is generally more efficient on military networks as it is connectionless (RFC768, 1980). This saves a lot of overhead at the cost of the application layer having to ensure that a full message can be reconstructed. The packets can arrive in any order or not at all and the higher level protocol must deal with this unlike TCP where the network stack will ensure packets are presented in order and losses are re-requested..

Some military Information Technology (IT) systems use UDP only for messaging and have proprietary application level services dealing with these issues. Whilst there is no accepted standard in the tactical domain, there are standards based protocols which could be used in place of TCP. Stream Control Transmission Protocol (SCTP) (Stewart, 2007) is an alternative to TCP and UDP. It has been shown to be more efficient for transporting web services over military networks (Johnsen, Bloebaum, Avlesen, Spjelkavik, Vik, 2013). SCTP support is not universal in Operating Systems (OS) and network devices. The advantages of SCTP will vary depending on the underlying network implementation.

The intelligent selection of protocols can also make the most efficient use of the underlying network at the application layer. Many modern systems use the Hypertext Transport Protocol (HTTP) to transfer data. Web browsing relies on HTTP as does the Simple Object Access Protocol (SOAP) which is commonly used to deliver Service Oriented Architecture (SOA). HTTP is delivered on top of TCP and thus has disadvantages on tactical networks. Google is producing a complimentary protocol called Quick UDP Internet Connect (QUIC) (Carlucci, De Cicco & Mascolo, 2015). This allows HTTP type data to be transferred over UDP and by doing so allows data to be multiplexed more easily. This is important for wireless transfers such as MANET as it allows the packets to be concatenated into larger frames for transmission. HTTP over TCP does not readily allow this as acknowledgement must first be received for a set window size of bytes. QUIC is not yet a standard but a sister protocol from Google for TCP called SPDY which has now been incorporated in to the recently released HTTP2 specification. In the assessed time-frame it is likely that QUIC or a successor will be more widely adopted.

Service Oriented Architecture

Enterprise architectures have made use of SOA for some time. It provides a level of abstraction and presents a common interface for the outside world. SOA architectures have only begun to be exploited in military computing at the strategic level of command (Zoughbi et al, 2011). The use of SOA in a more tactical environment is more challenging with near real time requirements and a restricted network (Saarelainen, Timonen, 2011). One key technology enabler for SOA is the Simple Object Access Protocol (SOAP). SOAP provides a standard way to describe and share information and services which allows different applications to connect without knowledge of the underlying data model.

SOAP can describe simple transactions and data but when dealing with more complex formats such as geographic information, they usually extend existing standards such as Geographic Markup Language (GML), Keyhole Markup Language (KML) or ESRI Shape files (Schnabel & Hurni, 2009). Applications used for Battle Management may support only a subset of these formats. Even with supported formats the implementation can vary which can potentially cause the data to lose fidelity. Therefore when using SOAP, data formats must be considered when selecting applications and for interoperability.

One way to resolve format issues and to structure information exchange is an Enterprise Service Bus (ESB) using a Publish/Subscribe model. An ESB provides another level of abstraction which among other things allows protocol conversion and data transformation (Chappell, 2004). This can consume data in multiple formats, normalise it, store it and send it on to subscribed applications. The Afghan Mission Network had such a service which was called the Publish and Subscribe (PaS) server. This concept has been taken forward and forms part of the Federated Mission Network concept (NATO Interoperability Standards and Profiles). An ESB is a complex software architecture but it provides flexibility and thus aids interoperability.

Semantic Web

One of the main benefits of an ESB approach is the ability to extract and search on semantic data. As the ESB ingests and normalises data it can hold it in a structured manner. It can then be drawn from multiple formats including human readable text. The data can be stored using the standard Resource Description Framework (RDF) and then searched using tools like SPARQL Protocol and RDF Query Language (SPARQL). This means other applications can understand and exploit it unambiguously based on shared ontologies. It also means that the ESB can be queried in a powerful way giving relevant results.

SOA and ESB provide many benefits but in the tactical domain can have severe drawbacks. If a central server was used then it could become a single point of failure and a bottle neck in the communications network. A tactical network should have system and geographic redundancy due to the effects of terrain and enemy action. SOA can be distributed across constrained networks and this can ensure access to information and remove pressure points from the data network (Ali, Hailong, Wei, 2013)

Applications

The choice of application will depend on the requirements and particular operation. This can change quickly due to the tactical environment or shared working with coalition partners. The key is to retain flexibility so that new applications can be incorporated quickly. This has proved difficult with monolithic C4 systems from defence vendors. As well as commercial lock in there are genuine concerns about system management and security when incorporating new software. Some mitigating techniques that can bring back flexibility are as follows:

Containerisation. Virtual Machines (VM) can be used to isolate instances of software but are quite a large overhead. A virtual machine runs a full OS and requires allocated memory and resources. This is possible especially when we consider Moore's law progress in the time-frame, however if each application has a full VM then this must be updated as well as the underlying OS. A lightweight modern solution is containerisation which uses the underlying OS but isolates the application environment (Dua, Raja, Kakadia, 2014). This means that applications and any dependencies can be updated without affecting others. It also keeps applications isolated so security concerns are reduced.

Open Source. The use of Open Source or Free Software can reduce costs when implementing a system but more importantly it provides greater freedom. If the source code is available then the system manager is not dependent on one vendor and their support. They also have the opportunity to analyse and improve the actual software. Whilst there is not a much military specific open source software use of standards based technologies discussed in this paper means that open source software can be adapted to the military need (Loechel, Mihelcic, Pickl, 2012).

Architectural approach

The above technology areas allow military requirements to be met but a system of systems approach is required to combine them to be a usable capability.

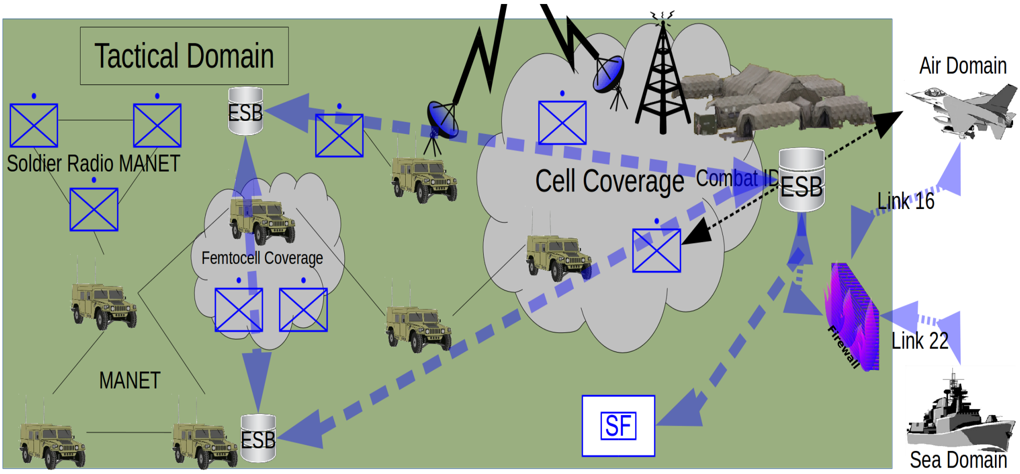

Fig 1: Candidate Architecture

The combination of these technologies is best done in a 'golf bag' type approach. This allows the technology to be combined in a way that matches the environment and meets the commanders needs for an operation. So for example in a fixed environment a COTS cell based communications can be used and linked straight back in to the strategic system. For more dynamic high intensity warfare a more militarised MANET communications network can be used with satellite based reach back to strategic systems.

The required applications can be drawn from those already integrated and trained or a specialist application can be easily incorporated. The ESB means a new application can more easily draw data from the wider system. This also makes interoperability easier with the ESB being able to transform the data and send out on another protocol. This for example could enable Air Land integration by sending the ground picture out on Link 16/22. Business rules can be applied for information release so potentially the system could even interface with other governments or Non Governmental Organisations.

Candidate Architectures

To illustrate the architectural approach and how some of the discussed technologies can be utilised a number of scenarios are discussed. A brief description of the scenario will be given along with a candidate architecture that could be deployed.

Software Architecture

The software architecture remains the same for all the scenarios. As in Fig 1 the architecture is layered on top of the networks discussed below. A federated ESB will be established to allow sharing of information with redundancy. Standard external linkages such as to the Air and Sea Domain will be already integrated and provided by an ESB.

Interoperability

Interoperability would be provided by the ESB in conjunction with firewalled touch points. The ESB will provide data normalisation to prevent unintended data leaking. The release of information can be implemented in the ESB by business rules or by positive release by a staff officer. Other external connections can be quickly specified and implemented using the ESB and a firewalled point of contact.

Protection of the home base from undeveloped adversaries

In this scenario operations are restricted to the countries own home base. The threat could be from subversive or state sponsored terrorists. The adversary does not have an advanced technological base but will make use of any available means to create an effect.

This architecture makes use of fixed infrastructure between the different headquarters and agencies (Fig 2). These will be wired links as part of the national infrastructure. Mobile units and temporary headquarters will be connected using a cell based infrastructure. This will be a combination of the nations safety networks which are presently usually based on Terrestrial Trunked Radio (TETRA) but in the time frame examined are likely to be a LTE or even 5g based safety networks. Where required capacity can be increased by using the civilian cell network. For those users in remote areas not covered by the cell network satellite means (both military and civilian) will be used.

This network will be very capable in terms of throughput and connectivity. The user will access using the same systems they are used to during peace time. The reliance on fixed infrastructure however does make it vulnerable to attack. Even a technologically disadvantaged opponent can target cell towers and other network infrastructure. This means that physical security will have to be enhanced in these sites which will cost manpower and equipment. The use of standard infrastructure would allow supporters for the opponent to mount cyber

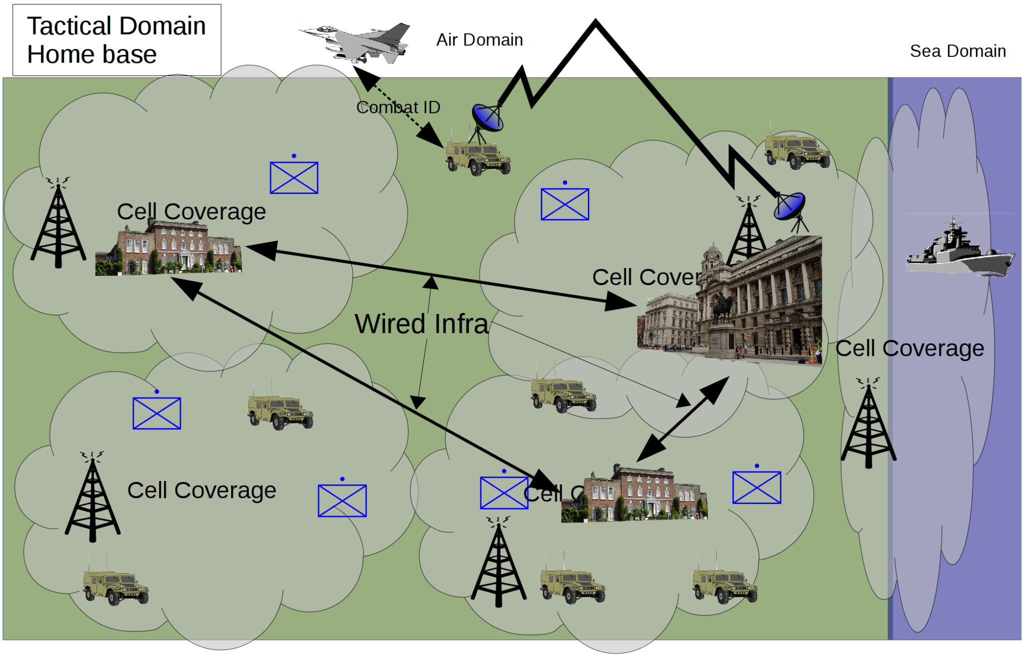

Fig 2: Protection of the home base from undeveloped adversaries

attacks. State sponsors would likely have the ability to have an effect but also 'hacktivist' groups can use known vulnerabilities to impede the network.

Protection of the home base from advanced adversaries

In this scenario operations still take place within the home base but against a more advanced adversary. This may be an invasion from another state or civil unrest supported by an advanced opponent.

The architecture takes a more hybrid approach and still uses some cell based and fixed infrastructure but supplements with more robust military communications (Fig 3). It is assumed the opponent will attempt to disrupt communications by kinetic and cyber means. The electromagnetic spectrum will be more contended with the enemy seeking to deny its use. A well equipped opponent will target vulnerabilities in cell based communications. This could lead to information being compromised or the network being blocked preventing information flow. Military communications systems will provide better Transmission Security (TRANSEC) and flexibility. In high intensity conflict the network will have to adapt quickly as the tactical units manoeuvre to gain advantage. MANET and connections to engineered links at the strategic level will allow the network to adapt to changing circumstances and enemy action.

This architecture provides a robust and adaptable network. It will not be able to offer the throughput or low latency of a fixed infrastructure. The entire network infrastructure will be organic to the tactical units and thus additional physical

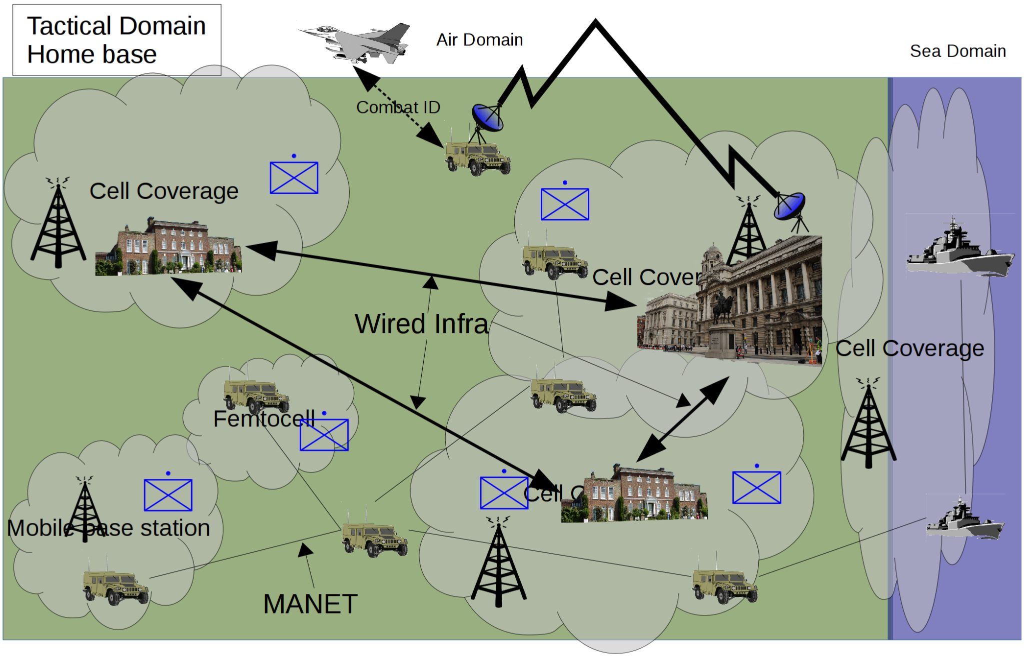

Fig 3: Protection of the home base from advanced adversaries

security will not be required. The cost of this specialised military equipment will be greater than utilising existing or commercially available equipment. To mitigate this smaller numbers may be bought for immediate action and training with an ability to quickly increase holdings during escalation to war.

Military operations outside the home base – low intensity

In this scenario a country is deploying forces outside its own borders. This would be for low intensity operations such as disaster relief, humanitarian or peace enforcement. The host nation, depending on how advanced they are, could have communications infrastructure. The infrastructure could be used in a benign environment but may be compromised due to disaster, an opponent or the number of other agencies trying to utilise them.

The architecture uses cell services where available but also allows military MANET where the force density and deployment allows (Fig 4). Satellite communications are used for reach back to the home base but also for disadvantaged users out with cell coverage or typical MANET distances.

The architecture for this sort of operation needs to be flexible as the situation will change. Fixed cell networks may not be accessible initially but may become available later. If many agencies or nations are in the area it will put great demands on infrastructure and spectrum availability. Whilst the generic software architecture remains the same, external connections to relief agencies or the host

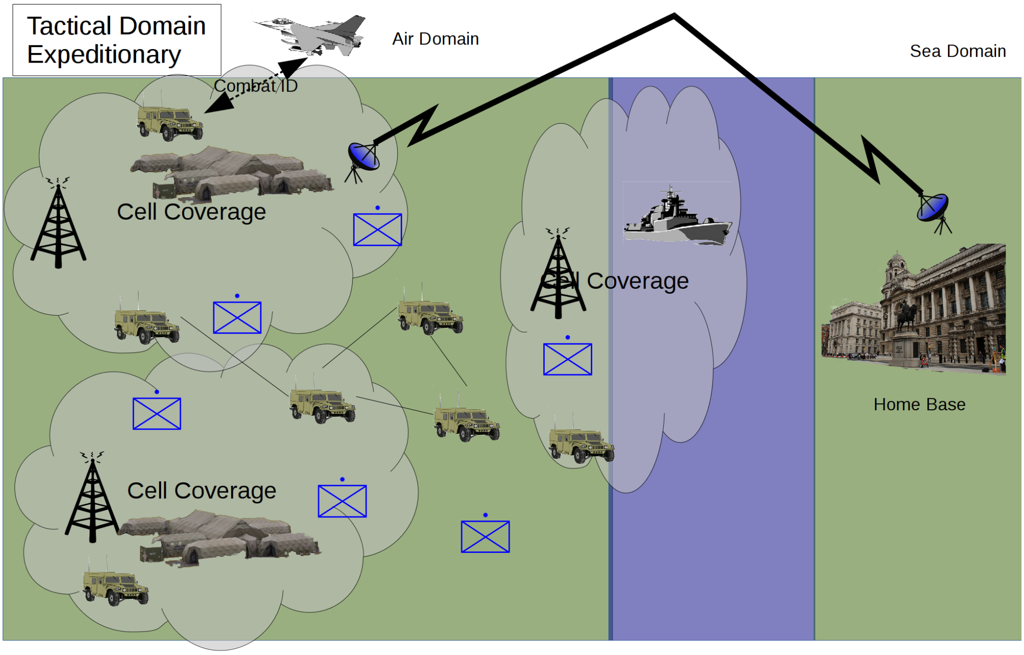

Fig 4: Military operations outside the home base – low intensity

nation may be required. This can be established by implementing the needed formats and protocols on the ESB and connecting via a firewalled connection.

Military operations outside the home base – high intensity

In this scenario a country is deploying a conventional force in to high intensity conflict in another area. This is likely to be as part of a coalition so interoperability is important. Access to any infrastructure or availability of spectrum is likely to be very limited. Enemy action and own forces manoeuvring will have a large impact upon network topologies. The enemy could be technically capable and hence the use of civilian infrastructure could have risks in terms of availability and cyber attack.

The architecture is mostly based on military off the shelf equipment but does allow a mix of cellular technology where the situation allows (Fig 5). The cell base stations could be deployed by the force as semi-permanent base stations of as mobile femtocells.

The reliance on military technologies will mean that throughput will be reduced from that provided in a more fixed infrastructure. The network should be more resilient to enemy action and to electronic warfare.

Other Lines of Development

The technology and the architecture presented will only become a usable system once the other lines of development are considered and developed.

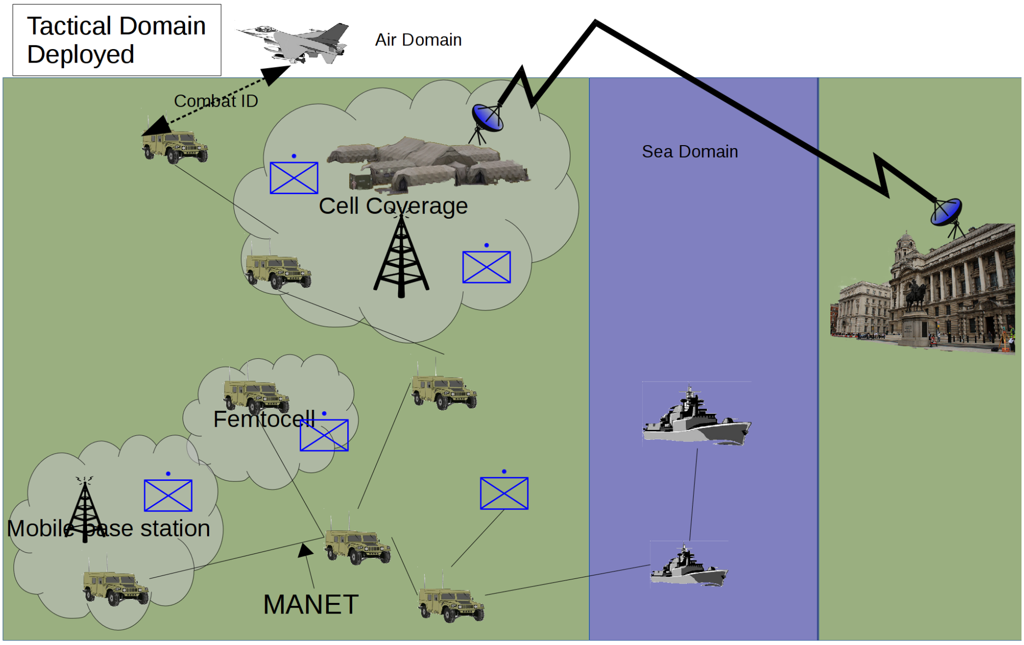

Fig 5: Military operations outside the home base – high intensity

Doctrine and training must allow the user to not only use but exploit the system to provide military capability. The system must be supported by a clear support strategy. Personnel must be properly trained and the lines of support documented and understood.

Transition to service can be very disruptive when new systems and ways of working are rolled out. The nature of the suggested technologies and the architectural approach lend themselves to a gradual roll out. The software architecture could be rolled out across a legacy data network. The use of the ESB can allow legacy applications to share data more easily with others on the system. This also allows benefits to be accrued early and avoid a disruptive transition.

The approach to the acquisition process must allow the same flexibility that is in the architectural approach. One vendor providing the entire solution, whilst simpler to contract, leads to vendor lock in and the pace and cost being set by that vendor. By ensuring open standards and with the use of open source technologies the right vendors can be selected for the given technologies. By favouring open source software it is also possible to change vendors mid development without losing the work already done.

This approach to acquisition requires an intelligent customer who understands the user need as well as the technology. Where possible this should come from within the military but when those skills are not available contractors separate and independent from the main suppliers should be used. It is important that the military should retain all the Intellectual Property (IP) and system ownership of the design and architecture.

Conclusions and future work

In this paper some of the key technology elements that could help specifying an independent tactical domain have been covered. The need for flexibility and independence from fixed solutions has been emphasised.

An architectural approach which provides a standards based network by the most efficient means for the tactical environment is proposed. The software layer has several methods to ensure flexibility as well as ease of implementation and maintenance. The use of containerisation ensures that applications are isolated and easily upgradable. The embedding of an ESB in the architecture ensures that data can be shared and structured for exploitation by semantic tools. It aids interoperability and makes the transition from legacy applications more seamless.

The technology itself is not sufficient to deliver military capability. The other elements must be considered and aligned with the technology development. An acquisition approach that retains as much IP and power within the military rather than a single selected vendor is preferred.

A number of candidate architectures were given as an example rather than a template as it is important for the commander and their J6 staff to retain flexibility. The scenarios show a range of intensities both in and out of the home base. Any operation will be unique with its own restrictions and requirements therefore the architecture will be planned based on matching the available capabilities.

Future work should look at the efficiency of the proposed technologies in a deployed tactical network. Particular emphasis should be put on a distributed architecture that avoids points of failure and makes efficient use of the underlying network.

References

Akyildiz, I.F. et al., 2008. A survey on spectrum management in cognitive radio networks. Communications Magazine, IEEE, 46(4), pp.40–48.

Ali, M., Hailong Sun & Wei Yuan, 2013. An Efficient Routing Scheme for Overlay Network of SOAP Proxies in Constrained Networks. In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. pp. 466–473.

Bard, J. and Kovarik Jr, V. J., 2007 Software defined radio: the software communications architecture. Vol. 6. John Wiley & Sons.

Bhattacharyya, B. & Bhattacharya, S., 2013, Emerging Fields in 4G Technology, its Applications & Beyond-An Overview. International Journal of Information and Computation Technology, Volume 3, Number 4 (2013), pp. 251-260

Carlucci, G., De Cicco, L. & Mascolo, S., 2015. HTTP over UDP: an Experimental Investigation of QUIC. In Proceedings of the 30th Annual ACM Symposium on Applied Computing. SAC '15. New York, NY, USA: ACM, pp. 609–614.

Chappell, D., 2004. Enterprise service bus, O'Reilly Media, Inc.

Clancy, T.C., Norton, M. & Lichtman, M., 2013. Security Challenges with LTE-Advanced Systems and Military Spectrum. In Military Communications Conference, MILCOM 2013 IEEE. pp. 375–381.

Dua, R., Raja, A.R. & Kakadia, D., 2014. Virtualization vs Containerization to Support PaaS. In Cloud Engineering (IC2E), 2014 IEEE International Conference on. pp. 610–614.

Goeller, L. & Tate, D., 2014. A Technical Review of Software Defined Radios: Vision, Reality, and Current Status. In Military Communications Conference (MILCOM), 2014 IEEE. pp. 1466–1470.

Ha, S.H. & Yang, J., 2013. Classification of switching intentions toward internet telephony services: a quantitative analysis. Information Technology and Management, 14(2), pp.91–104.

Hartman, A.R. et al., 2011. 4G LTE wireless solutions for DoD systems. In Military Communications Conference, MILCOM 2011. pp. 2216–2221.

Jarschel, M. et al., 2011. Modeling and performance evaluation of an OpenFlow architecture. In Teletraffic Congress (ITC), 2011 23rd International. pp. 1–7.

Johnsen, F.T. et al., 2013. Evaluation of transport protocols for web services. In Military Communications and Information Systems Conference (MCC), 2013. pp. 1–6.

Joint Capabilities Integration and Development System (JCIDS) Manual, 2012.

Johnsen, F.T. et al., 2013. Evaluation of transport protocols for web services. In Military Communications and Information Systems Conference (MCC), 2013. pp. 1–6.

McKeown, N. et al., 2008. OpenFlow: Enabling Innovation in Campus Networks. *SIGCOMM Comput. Commun. Rev.*, 38(2), pp.69–74.

Mitola, J., 1995. The software radio architecture. Communications Magazine, IEEE, 33(5), pp.26–38.

Mitola, J. & Maguire, G.Q., 1999. Cognitive radio: making software radios more personal. Personal Communications, IEEE, 6(4), pp.13–18.

NATO Interoperability Standards and Profiles, 2014, FMN Architecture, Available through: http://goo.gl/a03JIC

RFC768 - Postel, J., User Datagram Protocol, RFC 768, August 1980. (http://tools.ietf.org/html/rfc768)

RFC793 - Postel, J., Transmission Control Protocol, RFC 793, September 1981. (http://tools.ietf.org/html/rfc793)

Royer, E.M. & Chai-Keong Toh, 1999. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2), pp.46–55.

Saarelainen, T. & Timonen, J., 2011. Tactical management in near real-time systems. In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2011 IEEE First International Multi-Disciplinary Conference. pp. 240–247.

Schnabel, O. & Hurni, L., 2009. Cartographic web applications–developments and trends. In Proceedings of the 24th international cartography conference, Santiago.

Singh, R.K., Joshi, R. & Singhal, M., 2013. Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET). International Journal of Computer Applications, 68(4).

Stewart, R. (2007), "Stream Control Transmission Protocol", RFC 4960, Internet Engineering Task Force.

Tortonesi, M. et al., 2013. Enabling the deployment of COTS applications in tactical edge networks. IEEE Communications Magazine, 51(10), pp.66–73.

Vankka, J., 2005. Digital synthesizers and transmitters for software radio, Springer-Verlag New York, 2005, 359p.

Vankka, J., 2013. Performance of Satellite Gateway over Geostationary Satellite Links. In Military Communications Conference, MILCOM 2013 IEEE. pp. 289–292.

Zimmermann, H., 1980. OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection. Communications, IEEE Transactions on, 28(4), pp.425–432.

Zoughbi, G. et al., 2011. Considerations for Service-Oriented Architecture (SOA) in military environments. In 2011 IEEE GCC Conference and Exhibition (GCC). pp. 69–70.