AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

AIRPOWER IN THE INFORMATION AGE: EMBRACING TCP/IP WITHIN AIRBORNE NETWORKS

by

Major Nathan C. Stuckey, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Commander James K Selkirk Jr., USN

Maxwell Air Force Base, Alabama

April 2015

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Given the challenges posed by the Anti-Access Area Denial (A2/AD) threat, it is crucial for the military to possess agile and adaptive airborne networks. Current legacy airborne communication systems are not sufficient to meet this challenge due to the extreme limitations on the type of information that they can send combined with the lack of dynamic self-forming and adaptive characteristics need to operate in a non-permissive environment. In contrast, the Transmission Control Protocol/Internet Protocol (TCP/IP) model provides an open and adaptive construct that has proved successful at seamlessly connecting large numbers of users to a vast array of applications. Airborne TCP/IP communication systems within DoD are currently in the infancy with systems like the Tactical Targeting Network Technology (TTNT) and the Multi-Role Tactical Common Data Link (MR-TCDL) appearing from the research labs. The U.S. military is now at a critical junction where decisions made today will have an enormous impact on the information sharing capabilities that will be available in the future A2/AD fight. Senior leaders must resist the temptation to be complacent with the current systems and instead forge ahead with a modern information age communications paradigm. Failure to do so will lead to a military paralyzed by the fog a war in the A2/AD environment due to the inability to rapidly and reliably share information.

Airpower in the Information Age: Embracing TCP/IP within Airborne Networks

One of the most common digital messages transmitted among airborne platforms in the counterinsurgency fights in Afghanistan and Iraq was the message denoting the location of a train. Throughout the theater, common operating pictures in military headquarters contained maps with symbols for locomotives with rail cars. As military commanders looked at these digital maps, the train symbols were the most important feature. The appearance of new trains on the map would start a flurry of activity. Military aircraft would be vectored to the location on the map identified as a train. So what is going on here? Are trains really that important? Does Afghanistan really have that many railroads? Why was the location of trains more important than any other object on the ground?

The reality is that the military was using a train to denote a Troops in Contact situation. The digital communication systems were so inflexible and difficult to modify that there was no way to properly denote Troops in Contact. Instead, military members had to find an alternative message and settled on the message for a train since it was rarely used and was displayed as a capital T on some displays. This may be understandable as a short term fix, but in over a decade the military has been unable to update their communication systems to account for one of the most common situations in modern conflict.

The legacy digital communication links and computing systems on airborne platforms that were developed in the 1970s and 1980s ushered in a revolution in the way America conducts war. The United States military has become increasing reliant on the concept of net-enabled warfare to project military power. The importance of digital communications will continue to increase in the information denied environment that will exist due to future Anti-Access Area Denial (A2/AD) threats. However, the legacy communication and computer systems on airborne

military platforms that have served us well to this point are based on an outdated paradigm that does not take advantage of the information age revolution that began in the 1990s. Effective information sharing among airborne platforms is hindered by tightly coupled, proprietary, and obsolete communications protocols and computing systems. In order to meet the complex information sharing needs that will be required in the future A2/AD environment, the US Air Force must the embrace the modern Transmission Control Protocol/Internet Protocol (TCP/IP) networking paradigm in its tactical airborne networks.

Military Airborne Networking History

By the early 1990's, advancements in technology led to drastic changes in how the United States has conducted warfare. This upheaval in military capability has been dubbed the Revolution in Military Affairs (RMA).[1] The RMA was fueled by advancements in communications and computers. These advancements enabled two major capabilities: precision guided munitions and net centric warfare. The technological breakthrough of using satellites to transmit Positioning, Navigation, and Timing (PNT) information led to the Global Positioning System (GPS). Using the GPS system, munitions could be delivered with amazing procession so that the military was no longer talking about the number of sorties to destroy a target but rather the number of targets that could be destroyed per sortie. In addition, the advancements in computers and communication led to what is known as net-centric warfare. This ability to digitally link sensors, shooters, and C2 systems led to a revolution in situational awareness and dynamic targeting. Together these systems drastically improved combat effectiveness.

The first example of this new way of fighting was seen in the first Gulf War. The ability to network warfighting platforms together resulted in a synergistic capability in which the collection of military assets was greater than the sum of its parts. Sensor platforms like Airborne

Warning and Control System (AWACS) and Joint Surveillance Target Attack Radar System (JSTARS) were used to identify targets that were then engaged by separate platforms. The success of net-centric warfare in the Gulf War surprised even U.S. military planners. The US was able to find and severely degrade the Iraqi army from the air. Coalition ground forces were able to push Iraqi forces out of Kuwait with relative ease in a short 100 hour campaign. This was in sharp contrast to the 10,000+ casualties that U.S. military planners had expected in the war.

Net-centric warfare has become the standard way the U.S. military fights. In the current wars in Afghanistan and Iraq, the U.S. military has deployed a wide range of ISR platforms all transmitting data back to the Combined Air Operations Center (CAOC). Using a range of digital command and control systems within the CAOC, aircraft are dynamically tasked to engage targets as they are located. Joint Terminal Attack Controllers (JTACs) on the ground are able to digitally pass coordinates to close air support aircraft.

This ability to dynamically identify, target and engage enemy targets is outlined in Air Force Doctrine Annex 3-60 "Targeting".[2] This document describes the six phases of dynamic targeting: find, fix, track, target, engage, and assess (F2T2EA). This processing is commonly referred to as the "kill chain". While in some cases this process may play out on a single platform, typically multiple platforms digitally connected share information in real-time and collaboratively work to execute the kill chain. The following example demonstrates this concept. A JSTARS aircraft locates a vehicle convoy and then transmits the data to the Common Operating Picture (COP) in the CAOC. The CAOC tasks an Unmanned Aerial Vehicle (UAV) to gather more detailed info on the convoy. The sensor data from the UAV (which is being flown remotely), is transmitted back to the CAOC where intelligence analysts confirm the convoy as a hostile priority target. Using digital C2 systems in the CAOC, a B-1 is then digitally tasked to

engage the convoy. Coordinates are then digitally passed from the JSTARS aircraft to the B-1, which engages the targets using precision guided munitions.

The above is an example of net-centric warfare which has greatly reduced the time it takes to execute the kill chain, and in many cases allows time sensitive targets to be engaged that would have been impossible in the past. By compressing the kill chain, it allows the U.S. military to operate within the decision cycle of the enemy and defeat them before they have the chance to react. While the individual platforms get a lot of attention, it is the data links which connect the platforms that enable this method in which we conduct war.

A2/AD Information Environment

While not perfect, these data links have more or less worked in the permissive environment in which we have fought during the last 10 years. However, as we look to the future, it is likely that potential adversaries will use anti-access/area denial (A2/AD) strategies to deny the US military the ability to project its combat power. Military conflicts of the last 20 years have shown potential adversaries the folly in attacking the US force-on-force. Rather they seek asymmetric capabilities to attack our vulnerabilities. One of these vulnerabilities is the data links which enable the net centric way in which we fight.

In his article, “Delivering Air Sea Battle”, Admiral Mark Fitzgerald postulates that “operating in a highly contested electromagnetic environment” will be one of three main challenges facing the military in the future. In order to disrupt US military capabilities, he sees the enemy of the future attacking our communication links. In order to operate in these environments in the future, he advocates the development of “self-forming network architectures, both line of sight and wide area networks using surrogate air-breathing satellites and point-to-point laser or radio frequency satellite communications.” He declares that

investments in military digital networks have lagged behind the development of next generation weapons systems. Admiral Fitzgerald recommends that the network architecture be developed and the acquisition process started immediately.[3]

Lt Gen David Deptula also believes that the military's ability to command and control its forces is threatened. He believes that the enemy will threaten our communication links as well as our C2 facilities. In his recent article "A New Era for Command and Control of Aerospace Operations", Gen Deptula advocates for a "Combat Cloud" which would rely on "information-age technologies to enable highly interconnected, distributed operations". This combat cloud would rely on "highly distributed, self-evolving, and self-compensating network of networks." He envisions a future in which all platforms are able to seamlessly transfer data between each other using self-forming networks. [4]

Both Gen Deptula and Admiral Fitzgerald recognize the important of "nontraditional" ISR capabilities in the future A2/AD fight. Admiral Fitzgerald states that "every platform will be a sensor."[5] This sentiment is echoed by Gen Deptula when he notes that the F-22 and F-35 are not just fighters but flying sensors that are able to operate in a denied environment unlike many of the traditional ISR platforms.[6] They both see a future in which the contested environment makes traditional ISR much more difficult and the military will need to rely on fifth-generation platforms like the F-35 that are able to operate in the A2/AD environment as sensor platforms. In order to make this possible, it will be important to outfit these platforms with the proper communication links that will be able to distribute the high bandwidth data gathered by these sensors.

Similarly, in the future A2/AD environment the collaboration between sensor and shooter will become increasingly important. Gen Deptula describes a scenario in which sensors aboard

an F-35 are used to cue Aegis fleet missile defense batteries.[7] As part of the Systems of Systems Integration Technology and Experimentation program, DARPA proposes using swarms of small cheap UAVs to penetrate a non-permissive environment. The UAVs would be used to form a sensor net to locate components of a mobile integrated air defense system (IADS). The sensor data would be transmitted to a manned 5th generation aircraft like the F-35 in which an operator onboard would use this data to select targets. The target data would then be linked to a "missile truck" similar to a C-17 operating outside of the treat radius of the IADS. The missile truck would then launch a salvo of standoff munitions against the enemy IADS.[8] Many of these types of scenarios have been proposed by military thinkers in response to the challenges of the A2/AD environment, but the glue that holds it all together is the communication links. To make this type of warfare possible, the platforms must be connected by robust, flexible links with enough bandwidth to share vast amounts of sensor data along with the ability to remotely control UAVs and net-enabled munitions.

To meet the challenges posed by highly contested environments in 2030, the U.S. military needs to immediately invest in the capabilities that will enable digital communications between platforms in this difficult setting. In an effort to counter U.S. military capabilities, opposing forces will only become more dispersed, mobile, and difficult to locate. This will require the U.S. to maximize the number of sensors over target and quickly share this data with shooters. This will only increase the U.S. reliance on data link technologies in future combat. The challenges facing digital communications in the future must be analyzed, solutions identified, and technologies developed if the U.S. is to maintain its dominance on the battlefield.

Current State of Airborne Digital Communications – Link 16 Case Study

Currently the military describes its system of sharing data to and from aircraft platforms as "data links." The military has invested billions of dollars in a multitude of various data links. Some examples are Link 11, Link 16, Variable Message Format (VMF), Common Data Link (CDL), Situational Awareness Data Link (SADL), Multifunction Advanced Data Link (MADL), Intra Flight Data Link (IFDL) to name a few. These data links are used to share a vast array of information to include things like images, digital voice, text, self-reporting details about a platform (position, fuel status, weapon status, etc) and target data.

One of the main problems with current airborne digital communications is the highly coupled, proprietary, and inflexible nature. Some examples from Link 16 can be used to highlight these problems. Link 16 makes a good case study as it is by far the most widely used airborne data link and is characteristics are highly representative of the other legacy data links. Link 16 was developed in the 1970s and for that time frame was highly advanced. Link 16 became operational in the mid-1980s with the introduction of Class 1 and Class 2 terminals that were initially installed on C2 platforms like AWACS.[9] Despite being developed 30 years ago, Link 16 is still in the process of being rolled out to new platforms. The B-1 is currently being upgraded with Link 16 and the upgrade is on track to be completed by 2019.[10] It is estimated that Link 16 has been installed on 5000 platforms as of 2015.[11]

The fact that the currently used data links between airborne platforms are based on 40 year old technology has resulted in many major limitations when compared to modern advancements in networking. One major limitation is that Link 16 can only send J-series messages. Unlike modern digital messages such as IP packets which can encapsulate any type of digital message that you can imagine, J series messages are very inflexible and can only transmit

very specific types of data. Each message is specifically formatted with predefined fields with a prespecified number of bits that are encoded into predetermined patterns to convey specific information.[12]

To highlight the prespecified and inflexible nature of J-series messages, one only has to look at the structure. Since the field that indicates the type of message is a five bit number, there is a maximum of 32 types of J series messages (2^5=32). There is also a 3 bit field for sub message, so there can be up to eight different types of each message (2^3 = 8).[13] For example a J2.x message is a Precise Participant Location and Identification (PPLI). Basically a PPLI is a message generated by a friendly unit that reports its location and status. This type of message is further broken down by type. For example a J2.2 is an Air PPLI, a J2.3 is a Surface PPLI, a J2.4 is a Subsurface PPLI, a J2.5 is a Land Point PPLI, and J2.6 is a Land Track PPLI. Each one of these messages will then be further broken down to the bit level. For example a J2.2 contains specific fields for things like location, amount of fuel onboard, types of armaments carried. Each of these fields are predefined in the standard and you can only share these types of data. If you wanted to share some sort of information not contained in these predetermined fields you are out of luck.

Even more limiting is the fact that that data you can put into one of these fields is limited to set values. This is why in the opening example, a locomotive had to be used to identify a Troops in Contact location. One of the fields of a J3.5 Land Point/Track is what type of track it is. That field can only contain a number from 0 – 500. Each number corresponds to a different type of object on land. If you want to keep track of a target on land that is not one of the 500 predefined things, it is impossible. While whoever came up with the list thought to include a bicycle, they did not have the foresight to have a Troops in Contact point be included.

The fact that everything is predefined not only makes things very inflexible, but also very complicated. Mil-STD 6016 which defines the Link 16 standard is over 9,000 pages long. Large portions of the standard are devoted to defining what the individual fields of each message mean. Since everything is static, you end up with lots of tables defining what a certain number in a field corresponds to. For example, in addition to the 500 types of land tracks in the J3.5 message, there is also a field that describes what a land track is doing. This field can contain a number between 0 – 71 corresponding to predefined activities like engaging, advancing, escorting, etc. Again, if the action of the track doesn't fit one of the 71 activities, you won't be able to share what it is doing. The predefined types of J3.4 Surface Tracks makes the 500 types of J3.5 Land Tracks look puny. There are over 4000 types of surface tracks including long retired individual classes of Soviet ships.

You can imagine the difficulty in keeping the standard up to date. It is a never ending process to keep something like the 4000 types of ships that can be selected up to date. Since new types of ships are always being created and old ones retired, the standard is out-of-date from the second a revision is released. To add to the issue, it takes years between revisions to the standard.

From the above examples, it is clear the severe restrictions on the type of information that can be shared by current data link systems. It is absurd when you compare this type of digital communication system to the modern systems that we now enjoy thanks to the information age revolution. In a world in which you are only limited by your imagination in what you can share through blogs and social media, the military is limited to sharing things from predetermined lists among military airborne platforms. This type of system is incompatible with the complex

information sharing requirements that are required to effectively fight in the A2/AD fight of the future.

In addition to the severe limitations on the type of data that can be shared using current data links, they are constrained in the amount of bandwidth available due to outdated radio technology. For example, Link 16 uses a primitive Time Domain Multiple Access (TDMA) protocol to share available bandwidth[14]. The TDMA protocol is designed to deconflict in time when different clients transmit so that transmissions from different clients do not conflict and jam each other.

Link 16 breaks up time into 12 second periods called frames[15]. A 12 second frame consists of 1,536 times slots. A J-Series message, which was described above, is sent during each of these time slots. For each client in the network, it is preassigned during which of these 1,536 time slots it will transmit. This assignment is contained in the network design load (NDL). Since each of the 1,536 time slots has to be assigned to a participant in the NDL, they end up being very complicated documents. In addition, the NDL has to be individually loaded into each network participant after it is created.

For these reasons, it is not easy to change the NDL very often. For example, it is common for a Geographic Combatant Command (GCC) to update their NDL on around a yearly basis. Therefore, the NDL must include every platform that might possibly be in a GCC's area of operations over the next year. This results in the 1,536 time slots being broken up between hundreds of platforms, some of which may not even be currently in theater. At any one time, only a small fraction of these platforms may be flying, so the time slots for all of the other nonflying platforms go unused. Therefore, even if only two aircraft are currently a participant in a Link 16 network, rather than being able to use half the bandwidth, they are only able to use a

small fraction of the bandwidth since it must be split between every platform that may be part of the network over the next year.

As you can imagine, modern communications systems would not be possible using this type of archaic process to share bandwidth. Could you imagine if the LTE cellular signal had to be split between every cell phone that might possibly be connected to a cell tower? In the United States, the available bandwidth would have to be split 100 million ways making it impossible to do the things that have been made possible by the communications revolution like browsing the web, streaming video, etc. Thankfully, more modern protocols have been invented like Carrier Sense Multiple Access (CSMA) that allows bandwidth to be efficiently shared by the current participants in a network[16].

As more and more military platforms become networked and the information sharing requirements increase in the dynamic A2/AD environment of the future, it will be essential to adopt a communications architecture that makes efficient use of bandwidth and does not require network participants to be identified a year in advance. Dynamic networks with dynamic participants will be necessary for the agile sharing of information. It will be important to share bandwidth efficiently in order to transmit what data is required in the future to include high resolution video and imagery.

One of the main reasons for the difficulty in upgrading military data links to take advantage of technological advancement is their highly coupled nature. The radio hardware, the types of messages that can be sent, the underlining communications protocols, and the client applications are all tightly coupled into single systems that can't be broken up and upgraded separately. To continue the Link 16 example, if MIL-STD 6016 is updated to send a new type of J-series message, then all of the Link 16 radios, data link gateways, and aircraft computer

systems have to be updated to take advantage of the change. This tightly coupled and inflexible nature also means that each type of data link system can only send their respective proprietary message format. For example, Link 16 systems can only send J series messages, EPLRS systems can only send K-series messages, Link 11 systems can only sent M-series messages, etc. The highly coupled nature of military data link systems is in sharp contrast to the flexibility of the TCP/IP protocols.

The TCP/IP model

In the late sixties and early seventies there were a number of separate closed networks in existence, closely mirroring the current state of military data links. One of these was the ARPAnet which was a program by the Advanced Research Projects Agency (ARPA). ARPA was later renamed with the word Defense in front and is now commonly known as DARPA. ARPAnet consisted of 4 nodes in 1969, which were at UCLA, Stanford, UC Santa Barbara, and the University of Utah.[17] By 1972, ARPAnet had 15 nodes and the first e-mail program was deployed which was written by Ray Tomlinson of BBN. This initial deployment of ARPAnet would grow to 200 nodes by the end of the 70s, but was a single, closed network much like today's data link networks. Under the sponsorship of DARPA, Vinton Cerf and Robert Kahn developed a way to create a network of networks or what they called "internetting"[18]. This was done through the development of the TCP/IP protocols, which were deployed to ARPAnet on January 1, 1983 in which all clients shifted from the old protocols, creating the modern internet as we know it.[19]

The internet, as ARPAnet became known, exploded in the 1990s. This was enabled by the transfer of ARPAnet to the commercial sector along with the creation of a new internet application called the Web. The Web was created by Tim Berners-Lee between 1989 and 1991

and is made up of four parts: HTML, HTTP, a Web server, and a browser.[20] Throughout the 1990s, the internet grew exponentially from around 100,000 users to around 300 million people connected to the internet.[21] By the end of the 90s, the internet consisted of hundreds of different applications with the four main applications being: email, the Web, instant messaging, and peer-to-peer file sharing.[22]

Internet growth since the beginning of the 2000s has been dominated by smartphones and social media. Internet usage has continued to explode with many segments of the global population now having internet for the first time through a smartphone. The first billion of users was reached in 2005, the second billion in 2010, and the third billion in 2014.[23] The number of applications in use has exploded beyond the four applications listed above with the addition of app stores built into common operating systems like IOS, Android, and Windows. Much of the internet usage has shifted from web browsers to custom apps that are downloaded from the app stores. The number of apps available range in the millions and include a range of diverse types to include banking, games, social media, navigations, commerce, news, weather, personal assistants, etc. The internet has become so ubiquitous that it has changed the lives of a large portion of humanity even modifying how human interact on a social level.

The flexibility and openness of the TCP/IP model has enabled the rapid growth of the internet. It is this flexibility and openness of the TCP/IP model that has enabled the wide range of uses for digital communication that is hindered only by the imagination. The TCP/IP model is based on a concept of decoupled layers which helps simplify the complex nature of digital communications. Each of these layers is defined by network protocols. Protocols define how something is done. Network protocols define the formats of messages along with the procedures to transmit these messages. By relying on a modular design, each independent layer can be

modified without affecting the other layers. The layered design provides the agility to constantly update portions of a large and complex system at a manageable level. The TCP/IP model is built on five layers: the application, transport, network, link, and physical layers.[24]

The application layer consists of the network applications and the protocols that they use.[25] The beauty of the TCP/IP model is that there are a limitless amount of applications that can be developed. Applications that use TCP/IP include email, web browsers, and millions of dedicated apps like Instagram, Twitter, Facebook, banking apps, games, etc. Due to the modular and decoupled nature of the TCP/IP layers, the lower level layers do not care what type of application messages are being sent over them and do not restrict these messages to a fixed format.

The routers and switches that make up the internet could care less whether a Facebook update or a Netflix movie is being sent over them. This has allowed application developers to build whatever they can imagine without being limited by the underlining communications system. This is in great contrast to the data link systems currently being used to send messages to airborne platforms. As described earlier, these systems can generally only send one very specific type of message, i.e. J-series message in Link 16. This has greatly hindered the development of applications onboard military aircraft to one very specific application that utilizes that corresponding specific message.

The next layer is the transport layer. Two main protocols exist at this layer: TCP and User Datagram Protocol (UDP).[26] TCP connects network applications together to create an end-to-end connection between them. In addition, TCP takes the messages from the application layer and breaks long messages into manageable sizes. The application messages are stuffed or encapsulated into a TCP message called a segment. It also contains a flow control algorithm that

controls the sending rate of messages so that the network does not become clogged. Finally, TCP ensures reliable delivery of the application messages and resends any that are lost while being sent on the network. TCP is used for any messages that you want to be reliably delivered. UDP is a no-frills service which simply sends messages without the above services. It is used for real time applications like streaming video and voice in which it does not make sense to resend lost packs.

The network layer is the core of the TCP/IP stack. The network layer message is called a datagram which contains the TCP segment from the transport layer. [27] The IP exists in the network layer. There is only one IP and all participants in the network must use it. It uses IP addresses to identify the various participants on the network. Various routing protocols exist in the network layer to route the IP datagrams to the proper destination.

The transport and network layer and the corresponding TCP and IP are the heart of TCP/IP model. These layers are the glue that allows a wide range of application messages to be sent over various different types of communication channels like Ethernet, satellite, or Wi-Fi. The TCP/IP layers provide the abstraction that separates the application layer from the link/physical layers that make up the communication channels. It enables any type of application message to be sent over any type of communication link. This is in stark contrast to the data links used on military aircraft today in which only one type of application message can be sent by a specific communication link.

The individual communication links are made up of the link and physical layers.[28] The link layer message is called a frame and contains the datagram from the network layer. The frame is the message that is sent by the actual communication link. The physical layer sends the individual bits of the frame over things like copper wire, fiber optics, or wirelessly through the

air. Communication links that are made up of these two layers include things like Ethernet, 802.11 Wi-Fi, Bluetooth, and LTE cellular links. Again the agility and flexibility of the TCP/IP model allows a wide range of communication links to be used seamlessly together. A laptop can be connected to the internet through both Ethernet and Wi-Fi depending on which is available and the network applications are unaffected.

Together the five layers of the TCP/IP model provide a flexible structure that allows an endless number of applications to be sent by numerous types of communication links. The decoupled nature of the layers allows for changes to be made at one layer and the other layers are unaffected. This allows new applications to be developed without having to change anything else about the network. In addition, new types of communication links can be released without impacting the overall network. For example, there have been numerous versions of 802.11 Wi-Fi released over the last 10 years which have greatly increased the amount of bandwidth available. The flexibility enabled by the decoupled nature of the layers has led to a communication network that has been able to improve and evolve by incorporating technological advancements and new ideas. It has resulted in a network that is used by a large portion of the world's population and has become so ubiquitous that many everyday activities like banking and social communication now utilize TCP/IP networks.

This is in stark contrast to military airborne communication technologies which have remained largely unchanged since the 1970's with regard to capabilities. The tightly coupled nature of legacy military data links means that all of the things that are in the five layers of the TCP/IP are bundled together making it very difficult to update these data links to incorporate modern technology. The military needs an airborne communications framework that is flexible and responsive in order to meet the challenges posed by dynamic A2/AD environments of the

future. To do this, the military must retire the previous paradigm and embrace the TCP/IP model.

The military has largely embraced the TCP/IP model with respect to communications between fixed land based C2 facilities. Currently, military command and control (C2) facilities like Air Operation Centers (AOCs), Air Support Operations Centers (ASOCs), Control and Reporting Centers (CRCs), Army HQs, etc. and land based sensors like ground based radars are digitally connected using TCP/IP based communication links. However, this TCP/IP connectivity does not extend to the airborne platforms. This situation is similar to the "last mile" issue within the telecommunications industry in which high bandwidth fiber optic networks are installed throughout the nation, but users at home are not able to take advantage of these high speed networks because individual houses are still connected to the network using legacy copper wires. This results in the current situation in which TCP/IP connected ground based nodes in the military network can transmit a wide range of information between each other, while the airborne platforms are limited to the simplistic communications allowed by legacy data links.

To take advantage of these land based TCP/IP connections, the military developed the Joint Range Extension Application Protocol – C (JREAP-C), which transmits J-series Link 16 messages over TCP/IP links.[29] Since the flexibility of the TCP/IP model allows for any type of application messages to be sent, TCP/IP links can be used to send the J-series messages between TCP/IP connected nodes. Use of JREAP-C links has become so common that when C2 messages are sent to aircraft via Link 16 from land based C2 nodes like the AOC, the J-series messages typically are transmitted over multiple TCP/IP links until they reach a ground station within the AOR that contains a Link 16 terminal. At this point, the messages are then transmitted over Link 16 to the aircraft.

Even J-series messages transmitted between two aircraft may travel over a TCP/IP link by JREAP-C. When operating in mountainous regions like Afghanistan, multiple ground nodes are installed so that aircraft that are separated by ridge lines and do not have line-of-site connectivity can communicate. For example, two F-16s that are operating in different valleys are able to communicate even though they do not have line-of-site RF connectivity through the use of these TCP/IP connected ground nodes. The first aircraft will transmit the J-series message to the local ground node, which will relay the message to the other ground node over JREAP-C. That message will then be transmitted to the second aircraft by Link 16 to the second aircraft.

Security

One of the criticisms of embracing the TCP/IP model has been security. It is beyond the scope of this paper to explore cyber security in detail. However, when compared to legacy data link communication protocols, the TCP/IP protocols are neither more nor less secure. The vast majority of risk to TCP/IP enabled systems comes from being connected to the internet. Military systems connected to the same network as billions of users are the reason that unclassified networks like the Nonsecure Internet Protocol Router Network (NIPRNet) are inherently insecure. Connectivity works both ways. By allowing military users to access the public internet, systems on the public internet are able to access military systems. The military has also embraced standalone TCP/IP networks like the Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS) to transmit its most sensitive classified data to include up to Top Secret information. These networks are logically separated from the commercial internet through encryption and are inherently much more secure.

However, the discussion of whether legacy data links are more or less secure than TCP/IP links is largely a moot point. As discussed earlier, most legacy data link traffic travels through TCP/IP links at some point. Since legacy data link networks like Link 16 are currently connected to TCP/IP links, the entire network, to include the legacy data links, inherit the same security posture as the connected TCP/IP network. Currently, if the classified military TCP/IP networks are compromised that carry legacy data link messages, than the non-TCP/IP portion is comprised as well. Converting the "last mile" connections to TCP/IP would not significantly decrease the security posture, but would allow for a vast increase in information sharing capabilities to the distant airborne platforms.

The Way Forward

It is essential for the military to adopt flexible and adaptable communication links for its airborne platforms. The current data link situation is not acceptable and will not meet the needs of the future A2/AD environment. The most successful paradigm for digital communications by far has been the TCP/IP model that was originally developed by the U.S. military. Given the amount of investment the commercial sector invests into TCP/IP networks, it is unlikely that the US military could develop a competing communications system that would be able to match the technical innovation happening in the TCP/IP arena. Instead the military should leverage the technical innovations made by the commercial sector by adopting TCP/IP links for its airborne networking needs.

The military should invest in military specific airborne communication links that utilize the TCP/IP model. Adopting the TCP/IP model does not necessarily mean that the US military will be able to adopt commercial-of-the-self communication links for its aircraft. Commercial wireless communication links like Wi-Fi, LTE, and Wi-Max are not suitable to the airborne

A2/AD environment. The distances involved coupled with the unique maneuverability and speed of military aircraft requires custom wireless technologies. In addition, military communication links must be able to operate in the jamming environment that will result from electronic warfare in the A2/AD environment. The beauty of the TCP/IP model is that the military can make unique investments into communication links at the link and physical layers while still being interoperable with the overall framework.

The biggest exception to the general lack of adoption of TCP/IP enabled airborne communication links has been among the dedicated ISR platforms. ISR platforms like the U-2 use the Common Data Link (CDL) to transmit ISR data like imagery and video over broadband TCP/IP links. The CDL was developed in the late 1970s as a point to point link for transmitting ISR data.[30] In the mid-1990s, the CDL standard was modified to incorporate an IP enabled architecture. It operates at the Ku-band, is jam-resistant, and can transmit at up to 274 Mbps.[31] A miniaturized lightweight version called Tactical CDL (TCDL) has been developed that weighs 2.5 pounds. It can transmit at data rates up to 45 Mbps at a maximum distance of 150 nautical miles. It has been installed into UAVs like the RQ-7B Shadow and MQ-8B Fire Scout.[32],[33]

The biggest constraint prohibiting CDL from being a complete replacement to the current legacy data links being used on the bulk of airborne platforms is the point-to-point nature of the system. The current tactical data links like Link 16 are omnidirectional in nature allowing sent messages to be received by all of the participants in the network. While the high frequency nature of CDL allows for high bandwidths at long distances, it restricts the link to point-to-point communication between two nodes. While this works well when connecting an ISR platform to a ground station, it makes it impossible to simultaneously connect multiple participants. In addition, the two nodes must know the locations of each other prior to establishing a link in order

to point their directional antennas at each other. Finally, the directional nature of the antennas makes it difficult for maneuverable aircraft like fighters to maintain a directional link.

However, CDL may have a role as the backbone of a tactical communications network. The Multi-Role TCDL program (MR-TCDL) envisions using CDL links to connect less maneuverable aircraft together to form a TCP/IP based hub and spoke network in the sky. Possible platforms for MR-TCDL include C2 nodes like AWACS and JSTARS along with air refuelers, and dedicated communications aircraft like BACN. The system would be able to support up to four CDL links per platform to include a satellite link at bandwidths up to 274Mbps per link.[34] The multiple links allow for a hub and spoke design in which multiple aircraft, ground stations, and satellites can be linked together over TCP/IP links. Northrup Grumman demonstrated the MR-TCDL capability during a 10-day exercise in Guam in September of 2010 called Valiant Shield. The system was flown on a Gulfstream II and connected to both a satellite and ground stations.[35] The Navy is currently engaged in an effort to install MR-TCDL on the E-6B, which is an airborne command and control platform for nuclear forces. The effort is scheduled to be completed by FY17.[36]

Another TCP/IP based airborne communication link under development is the Tactical Targeting Network Technology (TTNT). TTNT is an airborne communication network that has a maximum throughput of 10 Mbps at a range of 300nm onboard an aircraft travelling up to Mach 8.[37] TTNT was developed by DARPA and first demonstrated in 2005 at China Lake, California and involved several platforms to include: F-15E, F/A-18, E-2C, Lear 25, T-39, Boeing 707, a surrogate CAOC and three mobile ground nodes.[38] While the maximum bandwidth is significantly less than CDL, it is omnidirectional which makes it more ideal for maneuverable aircraft like fighters. The omnidirectional nature also lets multiple participants

easily join and participate in the network unlike point-to-point solutions with directional antennas which can only connect to one other node. In addition, the omnidirectional nature allows TTNT to link with multiple users on the ground and could be used in mission sets like digital close air support (CAS). TTNT could also be used to control multiple network enabled weapons. TTNT could also enable scenarios in which the weapon is controlled by a node other than the shooter. For example, a weapon could be dropped and control of the weapon could be handed off to a JTAC on the ground.

The range and omnidirectional nature of TTNT makes it a good replacement for current tactical airborne data links like Link 16. Development of TTNT has continued albeit at a slow pace. It was demonstrated on an F-22 during the Joint Expeditionary Force Experiment 2008.[39] In 2013, TTNT was demonstrated onboard the X-47B, the Navy's experimental Unmanned Combat Air System.[40] In August of 2014, the Navy awarded a contract to integrate TTNT into the Multifunctional Information Distribution System Joint Tactical Radios System (MIDS JTRS) terminal which is expected to be completed by August 2017. The MIDS JTRS terminal is the latest version of the MIDS Link 16 terminal.[41] If this effort is successful, then the MIDS JTRS terminal would be able to transmit both the Link 16 and TTNT waveforms.[42]

The current state of TCP/IP based airborne networking mirrors the state of legacy data links in the 1980s. The deployment of legacy data links like Link 16 has taken over 30 years and is still ongoing, as can be seen by the B-1s not being fully operational until 2019. To date, the deployment of TCP/IP data links has proceeded slowly as TCP/IP data links like TTNT are still in the developmental phase more than 10 years after being initially demonstrated. To meet the challenges of the future A2/AD environment, the military cannot delay further.

As discussed earlier, the future A2/AD environment will force the military to rely on non-traditional ISR from "tactical" platforms like the F-22 and F-35. In addition, many of the proposed scenarios enabling the military to operate in an A2/AD environment rely on collaboration between various sensor and shooter platforms. Concepts like DARPA's Systems of Systems Integration Technology and Experimentation program, in which swarms of UAVs transmit target coordinates to missile trucks, can only be achieved through the use of modern information age communication links. Even with the full backing of the military, deploying a new modern TCP/IP based airborne network will take time. If the A2/AD concepts proposed by the military community are to be made a reality by 2040, the military must engage in a full fledge effort to replace the legacy non-TCP/IP links with a modern replacement.

Conclusion

Given the challenges posed by the A2/AD threat, it is crucial for the military to possess agile and adaptive airborne networks. As identified by senior leaders like General Deptula and Admiral Fitzgerald, communication systems that can send a wide range of diverse information and dynamically operate in an A2/AD environment will be an essential ingredient to successfully conducting war in the future. Current legacy airborne communication systems are not sufficient to meet this challenge. Legacy data links are very limited in the type of information that they can send. In addition, legacy systems lack the dynamic self-forming and adaptive characteristics need to operate in a non-permissive environment. In contrast, the TCP/IP model provides an open and adaptive construct that has proved successful at integrating technological advancements. The TCP/IP has also demonstrated the ability to seamlessly connect a large number of participants, to include networks of over a billion clients, to a wide range of different applications.

Given the information sharing requirements necessary to operate in the A2/AD environments of the future, the military cannot take 30 years to connect its airborne platforms through TCP/IP networks. Tactical airborne TCP/IP links will be an essential requirement to give platform engineers the flexibility to design the applications necessary to wage war in an A2/AD environment. The ability to exchange information between airborne platforms unconstrained by the underlining communication systems is a key ingredient enabling the advanced A2/AD concepts proposed by military thinkers.

Airborne TCP/IP communication systems within DoD are currently in the infancy with systems like TTNT and MR-TCDL appearing from the research labs. The U.S. military is now at a critical junction where decisions made today will have an enormous impact on the information sharing capabilities that will be available in the future A2/AD fight. It will be crucial for the DoD to embrace these types of TCP/IP enabled systems and develop a deliberate and comprehensive deployment plan. Senior leaders must resist the temptation to be complacent with the current systems and instead forge ahead with a modern information age communications paradigm. Failure to do so will lead to a military paralyzed by the fog a war in the A2/AD environment due to the inability to rapidly and reliably share information.

Endnotes

[1] Steven Metz and James Kievit. Strategy and the Revolution in Military Affairs. Carlisle Barracks, PA.: Army War College, 27 June 1995, 4.
[2] Air Force Doctrine Annex 3-60, Targeting, 10 January 2014, 46-48.
[3] Mark P. Fitzgerald. "Delivering Air Sea Battle." JFQ 67 (4th Quarter 2012), 54.
[4] David A. Deptula. "A New Era for Command and Control of Aerospace Operations." Air & Space Power Journal, July-August 2014, 11.
[5] Mark P. Fitzgerald "Delivering Air Sea Battle." JFQ 67 (4th Quarter 2012), 55.
[6] David A. Deptula. "A New Era for Command and Control of Aerospace Operations." Air & Space Power Journal, July-August 2014, 8.
[7] Ibid.
[8] Defense Advanced Research Projects Agency. "Operating in Contested Environments." http://www.darpa.mil/NewsEvents/Releases/2015/03/30.aspx.
[9] *Understanding Voice and Data Link Networking: Northrop Grumman's Guide to Secure Tactical Data Links*. San Diego, CA: Northrop Grumman, December 2013, 2-3.
[10] Staff Sgt. Joel Mease. "Link 16: The B-1B's future link to the battle field" *Dyess Air Force Base*, 9 April 2014. www.dyess.af.mil/news/story.asp?id=123406697.
[11] *Understanding Voice and Data Link Networking: Northrop Grumman's Guide to Secure Tactical Data Links*. San Diego, CA: Northrop Grumman, December 2013, 2-2.
[12] Ibid., 2-7.
[13] Ibid.
[14] Ibid., 2-31.
[15] Ibid., 2-34.
[16] James F. Kurose, and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet (Third Edition).*Boston, MA: Pearson/Addison Wesley, 2005, 435.
[17] Ibid., 53.
[18] Ibid., 54.
[19] Ibid., 56.
[20] Ibid., 57.
[21] Internet Live Stats. "Internet Users." http://www.internetlivestats.com/internet-users/.
[22] James F. Kurose, and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet (Third Edition).*Boston, MA: Pearson/Addison Wesley, 2005, 57.
[23] *The World in 2014.* ICT Facts and Figures. Geneva, Switzerland: International Telecommunication Union, April 2014.
[24] James F. Kurose, and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet (Third Edition).*Boston, MA: Pearson/Addison Wesley, 2005, 47.
[25] Ibid., 48.
[26] Ibid.
[27] Ibid., 49.
[28] Ibid.
[29] *Understanding Voice and Data Link Networking: Northrop Grumman's Guide to Secure Tactical Data Links*. San Diego, CA: Northrop Grumman, December 2013, 7-6.
[30] D. Curt Osterheld. *Common Data Link Overview,* Seventh International Data Links Symposium, Washington, DC, 16-18 October 2007, 26.

[31] Ibid., 28, 39, 41.
[32] Brandie Woodard. “Miniature Common Data Link Transitioned” *Wright-Patterson Air Force,* 2 April 2012, http://www.wpafb.af.mil/news/story.asp?id=123296338.
[33] L-3 Communications. “Mini TCDL Transceiver data sheet.” http://www2.l-3com.com/csw/ProductsAndServices/DataSheets/Mini-TCDL_Transceiver_Sales-Sheet_WEB.pdf.
[34] L-3 Communications. “Multi-Role Tactical Common Data Link data sheet.” http://www2.l-3com.com/csw/ProductsAndServices/DataSheets/MR-TCDL_Product_Line_Sales-Sheet_WEB.pdf.
[35] Globe Newswire. “Northrop Grumman Successfully Demonstrates MR-TCDL Capabilities During Valiant Shield Exercise.” *NBC News,* 9 December 2010. http://www.nbcnews.com/id/40590218/ns/business-press_releases/t/northrop-grumman-successfully-demonstrates-mr-tcdl-capabilities-during-valiant-shield-exercise/#.VRMPMnkcTec.
[36] Federal Business Opportunities. “E-6B MR-TCDL Solicitation Number: N00019-12-C-0096” https://www.fbo.gov/?s=opportunity&mode=form&id=199ead28d9c7410279d04aa8bcb78e8e&tab=core&_cview=0.
[37] Rockwell Collins. “Tactical Targeting Network Technology data sheet.” https://www.rockwellcollins.com/~/media/Files/Unsecure/Products/Product%20Brochures/Communcation%20and%20Networks/Networks/Tactical%20Targeting%20Network%20Technology/TTNT%20brochure.aspx.
[38] “DARPA Successfully Demonstrates Tactical Targeting Network Technology.” *Deagel.com,* 24 October 2005. http://www.deagel.com/news/DARPA-Successfully-Demonstrates-Tactical-Targeting-Network-Technology_n000000559.aspx.
[39] Air Combat Command Public Affairs. “JEFX 08 demonstrates F-22 Raptor sensor capabilities.” *Air Combat Command,* 13 May 2008. http://www.acc.af.mil/news/story.asp?id=123098412.
[40] Rockwell Collins. “Rockwell Collins supplies Tactical Targeting Network Technology for deck handling trials of X-47B Unmanned Demonstrator.”, 20 March 2013. http://www.rockwellcollins.com/sitecore/content/Data/News/2013_Cal_Yr/GS/FY13GSNR20-X47B.aspx.
[41] ViaSat. “Multifunctional Information Distribution System Joint Tactical Radio System data sheet.” https://www.viasat.com/files/assets/web/datasheets/MIDS_JTRS_datasheet_035_web.pdf
[42] U.S. Department of Defense. “Contracts for August 19, 2014.” http://www.defense.gov/contracts/contract.aspx?contractid=5355

Bibliography

Air Combat Command Public Affairs. "JEFX 08 demonstrates F-22 Raptor sensor capabilities." *Air Combat Command,* 13 May 2008. http://www.acc.af.mil/news/story.asp?id=123098412.

Air Force Doctrine Annex 3-60, Targeting, 10 January 2014.

"DARPA Successfully Demonstrates Tactical Targeting Network Technology." *Deagel.com,* 24 October 2005. http://www.deagel.com/news/DARPA-Successfully-Demonstrates-Tactical-Targeting-Network-Technology_n000000559.aspx.

Defense Advanced Research Projects Agency. "Operating in Contested Environments." http://www.darpa.mil/NewsEvents/Releases/2015/03/30.aspx.

Deptula, David A. "A New Era for Command and Control of Aerospace Operations." *Air & Space Power Journal*, (July-August 2014): [5-16].

Federal Business Opportunities. "E-6B MR-TCDL Solicitation Number: N00019-12-C-0096" https://www.fbo.gov/?s=opportunity&mode=form&id=199ead28d9c7410279d04aa8bcb78e8e&tab=core&_cview=0.

Fitzgerald, Mark P. "Delivering Air Sea Battle." *JFQ* 67 (4th Quarter 2012): [53-55].

Globe Newswire. "Northrop Grumman Successfully Demonstrates MR-TCDL Capabilities During Valiant Shield Exercise." *NBC News,* 9 December 2010. http://www.nbcnews.com/id/40590218/ns/business-press_releases/t/northrop-grumman-successfully-demonstrates-mr-tcdl-capabilities-during-valiant-shield-exercise/#.VRMPMnkcTec.

Internet Live Stats. "Internet Users." http://www.internetlivestats.com/internet-users/.

Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet (Third Edition).*Boston, MA: Pearson/Addison Wesley, 2005.

L-3 Communications. "Mini TCDL Transceiver data sheet." http://www2.l-3com.com/csw/ProductsAndServices/DataSheets/Mini-TCDL_Transceiver_Sales-Sheet_WEB.pdf.

L-3 Communications. "Multi-Role Tactical Common Data Link data sheet." http://www2.l-3com.com/csw/ProductsAndServices/DataSheets/MR-TCDL_Product_Line_Sales-Sheet_WEB.pdf.

Mease, Staff Sgt. Joel. "Link 16: The B-1B's future link to the battle field" *Dyess Air Force Base*, 9 April 2014. www.dyess.af.mil/news/story.asp?id=123406697.

Metz, Steven, and James Kievit. *Strategy and the Revolution in Military Affairs*. Carlisle Barracks, PA.: Army War College, 27 June 1995.

Osterheld, D. Curt. *Common Data Link Overview,* Seventh International Data Links Symposium, Washington, DC, 16-18 October 2007.

Rockwell Collins. “Rockwell Collins supplies Tactical Targeting Network Technology for deck handling trials of X-47B Unmanned Demonstrator.”, 20 March 2013. http://www.rockwellcollins.com/sitecore/content/Data/News/2013_Cal_Yr/GS/FY13GSNR20-X47B.aspx

Rockwell Collins. “Tactical Targeting Network Technology data sheet.” https://www.rockwellcollins.com/~/media/Files/Unsecure/Products/Product%20Brochures/Communcation%20and%20Networks/Networks/Tactical%20Targeting%20Network%20Technology/TTNT%20brochure.aspx.

Understanding Voice and Data Link Networking: Northrop Grumman’s Guide to Secure Tactical Data Links. San Diego, CA: Northrop Grumman, December 2013.

U.S. Department of Defense. “Contracts for August 19, 2014.” http://www.defense.gov/contracts/contract.aspx?contractid=5355

ViaSat. “Multifunctional Information Distribution System Joint Tactical Radio System data sheet.” https://www.viasat.com/files/assets/web/datasheets/MIDS_JTRS_datasheet_035_web.pdf

Woodard, Brandie. “Miniature Common Data Link Transitioned” *Wright-Patterson Air Force*, 2 April 2012, http://www.wpafb.af.mil/news/story.asp?id=123296338.

The World in 2014. ICT Facts and Figures. Geneva, Switzerland: International Telecommunication Union, April 2014.