ADLINK
Leading EDGE COMPUTING

DDS at the Tactical Edge Whitepaper

www.adlinktech.com
2017

Table of Contents

1. Computing Trends in Defense Systems

The concept of network centric warfare was pioneered by the United States, but has been subsequently adopted as military doctrine by other countries worldwide. The idea is that battlefield advantage can be gained through a network of robustly connected forces to improve information sharing, which in turn improves situational awareness and decision-making responsiveness, dramatically improving mission effectiveness.

The U.S. is developing the Global Information Grid (GIG) as the primary communication framework to support network centric warfare operations. The GIG is a globally interconnected, end-to-end set of information capabilities for sensing, collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel.

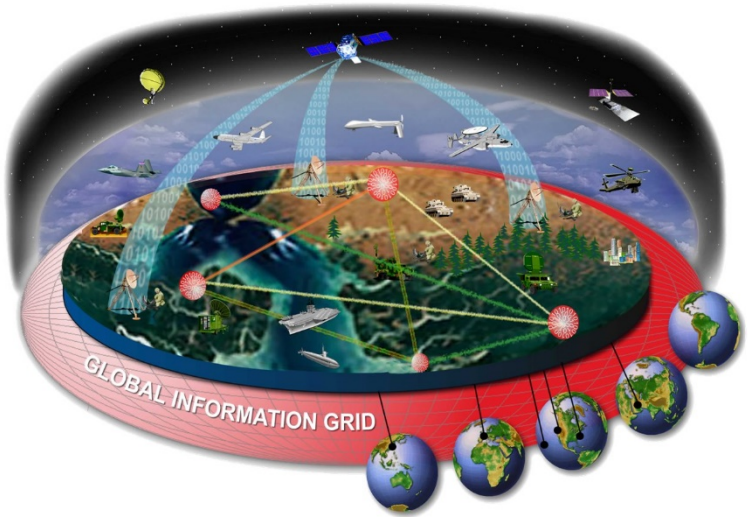

Figure 1 – Global Information Grid

The military strategist and U.S. Air Force Col. John Boyd developed the decision cycle of Observe, Orient, Decide and Act (OODA loop). The idea being that an entity, whether an individual or an organization, can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent and thereby "get inside" the opponent's decision cycle and gain the advantage. Fundamental to the effectiveness of the decision cycle and embraced by the doctrine of network centric warfare is being able to deliver the right data, at the right place at the right time. This is key to reducing the time to make good command decisions and gain advantage.

In a network centric environment consisting of a geographically dispersed and interconnected system of systems, the collection, storage, processing and dissemination of information represents a major technical challenge. The use of cloud and edge computing in a military context, combined with use of real-time data connectivity enabled by the Object Management Group's Data Distribution Service (DDS) standard, offers great potential to effectively address these hurdles.

Another set of concerns relate to the sheer volume, variety and velocity of data produced by network centric military applications that has grown exponentially in the past decade. This poses many challenges with respect to how to manage, process and share the data in systems containing edge networks, limited computing resources, limited network bandwidth and where connectivity to centralized command and control systems is not always guaranteed.

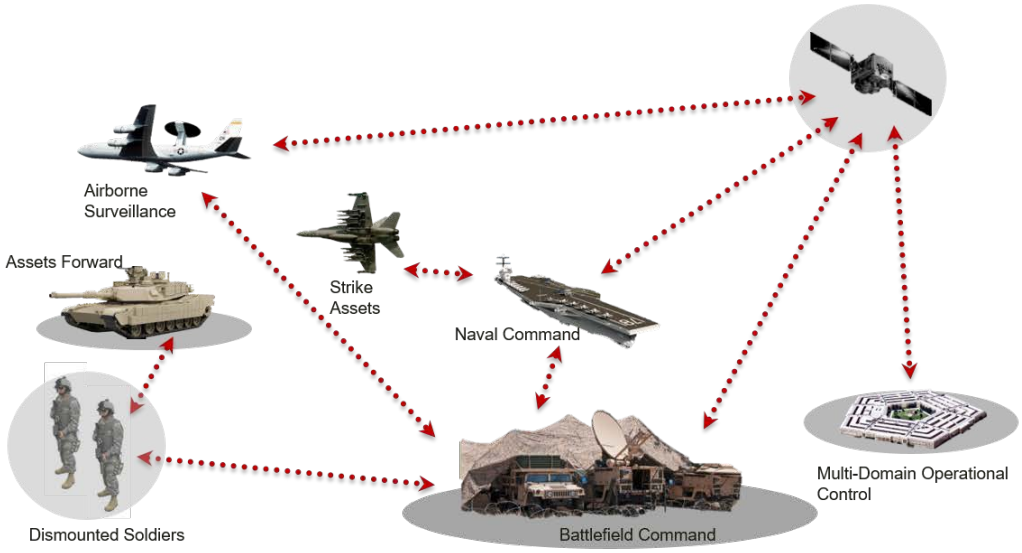

Figure 2 – Network Centric System of Systems

2. Cloud Computing in Defense

To support future network centric warfare systems, the U.S. Department of Defense has started a number of initiatives aimed at achieving improved mission and cost effectiveness. One of the key initiatives is to accelerate the adoption of cloud computing.

The objective is to move from a state of duplication, cumbersome and costly application siloes to a much more cost effective and agile service environment that can rapidly respond to changing mission requirements. Cloud computing can enhance battlefield mobility through device and location independence while providing on-demand secure global access to mission data and enterprise services. It is worth pointing out that the DoD has specific requirements for the adoption of cloud computing technologies in areas such as cyber security, continuity of operations, information assurance and resilience that both government and commercial providers must comply with.

Figure 3: DoD Enterprise Cloud Environment[1]

[1] Chief Information Officer, Cloud Computing Strategy, July 2012

Cloud computing relies on applications, storage and computing that reside on networks with powerful servers and not necessarily on local machines that can have far less computational power. Cloud computing enables thin clients such as a mobile device to access the computing resources of servers in a cloud data center.

The cloud computing paradigm works effectively until you get to the tactical edge, such as on the battlefield where mission requirements are dynamic and fast changing, and where the need for computing power is great but network communications are much more challenging. Specifically, due to intermittent connectivity with the core networks, limited network bandwidth and high network latency.

3. Edge Computing & Tactical Cloudlets

Cloudlets address the limitations of cloud computing at the tactical edge. Cloudlets consist of servers and communication equipment that are deployed on the battlefield, typically hosted on a vehicle or other platforms in the proximity of the troops. They offer computational offload capabilities to mobile forces, forward data staging for a mission, provide data filtering for streams intended for dismounted users and also are a collection point for data heading to the cloud or other battlefield edge nodes.

Tactical Cloudlets can continue to be used even if disconnected from the core network. The offloading of computational tasks from resource-poor mobile devices to more powerful machines in the vicinity is termed cyber foraging.

The key elements of the Cloudlet architecture include:

- The servers are forward deployed, for example, on the battlefield much closer to the troops.
- The servers are discoverable, which is fundamental to how users access the services they provide. Users are able to discover the services they require at runtime without knowing the exact IP address of these applications in advance.
- The servers are typically Virtual Machine (VM) based so that computational resources and applications can be provisioned on demand.

They can operate in a fully disconnected mode, with connection to the cloud only required in some types of provisioning scenario, for example, if VMs and apps hosted in local Cloudlet repositories need to be updated because newer versions have been made available.

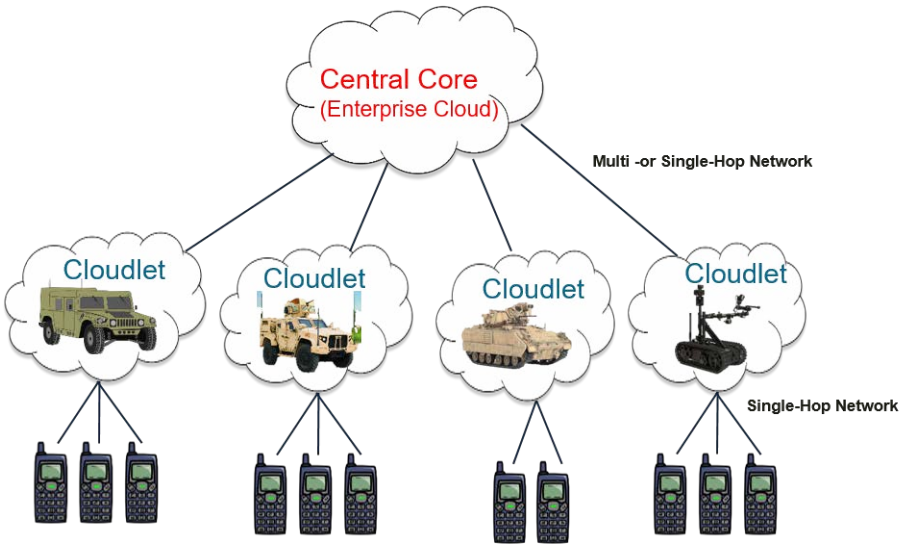

Figure 4 – Tactical Cloudlets [2]

[2] Carnegie Mellon University. Tactical Cloudlets, Grace A. Lewis – Dec 10, 2014

Fundamental to supporting tactical edge networks using Cloudlets is the need for a discovery service, used in combination with a provisioning and execution infrastructure for virtualized servers and applications.

Another extremely important aspect of these edge-based tactical networks is the ability to share data in real time between a dynamic network of ad-hoc nodes that may come and go over time. To support a shared operational picture and effective decision making, a peer-to-peer communication fabric that also removes singles points of failure is key.

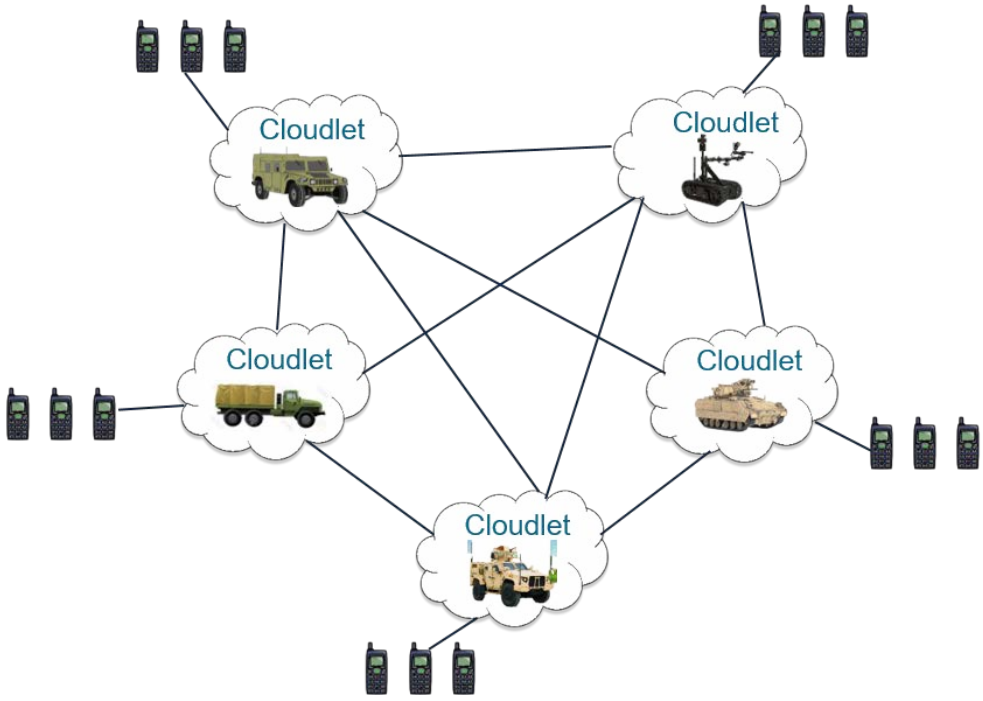

Figure 5 – Peer-to-Peer Communications

The need for network centric military systems to efficiently offload computational workload at the edge, to process data locally and to share information with nodes and users in close proximity has many synergies with the requirements for business-critical Internet of Things (IoT) systems, particularly in an industrial context. For example, cloud computing is already pervasive in Machine-to-Machine (M2M) industrial applications and where similar challenges also exist with the limitations of cloud-centric architectures in the IoT. This is also driving the need to deploy computing resources much closer to the data sources, for localized processing and decision making.

Conceptually the tactical cloud architecture shares many similarities to the edge computing concept, also commonly referred to as fog computing in the Industrial IoT world, and which is supported by international standards bodies such as the OpenFog Consortium and also ETSI, who is developing a Mobile Edge Computing (MEC) architecture for the mobile telecommunications industry. The important point being that technologies that are being developed for the IoT and for network centric tactical edge systems have massive synergy and dual use. This means that IoT technologies developed in the commercial world are capable of supporting initiatives such as the DoD's third offset strategy with its focus on increased use of COTS technologies where applicable.

4. Critical Software for the Tactical Edge

When the GIG was originally proposed, the distributed technologies of the day, such as CORBA and COM/DCOM, were not particularly well-suited to its implementation. The request-and-reply style of interaction supported by technologies such as CORBA resulted in tightly coupled systems that introduced single points of failure and bottlenecks, which in turn led to systems that were difficult to scale, prone to faults and had performance issues.

The DDS standard was developed by the Object Management Group and its member companies to address the limitations of existing client-server technologies for addressing the communication and real-time data sharing challenges of the GIG.

DDS was introduced as a OMG standard in 2004 and continues to evolve to this day, with recent additions to the set of standards, including support for a comprehensive pluggable security framework, extensible data types and RPC-style interactions. DDS defines an interoperable wire protocol referred to as DDSI and a set of language-independent, data-centric APIs that support a publish and subscribe interaction style. DDS provides interoperable, QoS controlled real-time data sharing for distributed systems.

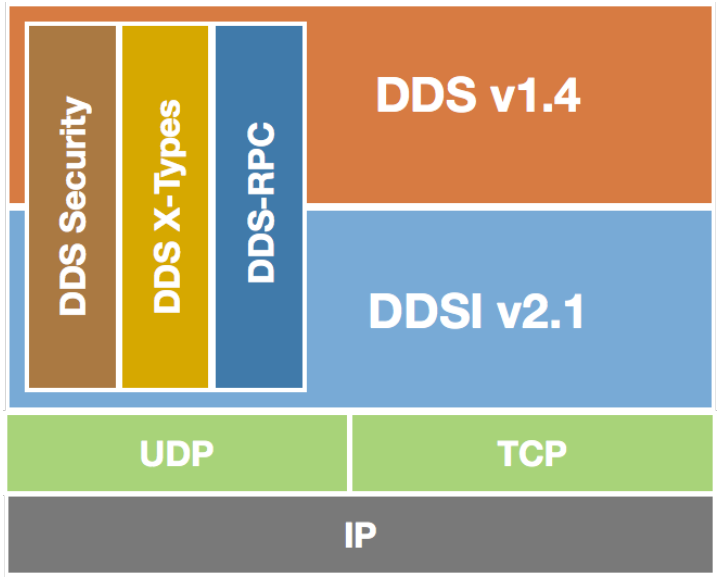

Figure 6 – OMG DSS Standards

DDS has recently been recommended as a core communication standard as part of the Industrial Internet Consortium's (IIC) Reference Architecture. DDS provides a Distributed Data Space abstraction where nodes can asynchronously read and write data into the data space regardless of their location. Readers and writers are decoupled in time and space and the data space is completely decentralized, reducing single points of failure. Data sharing interactions are controlled by a rich set of QoS polices. The built-in discovery mechanism allows applications to easily discover each other regardless of location and network topology.

So why DDS for network centric military systems? Just to reiterate the point again, DDS is a standard designed for network centric systems and with its original focus very much on the aerospace and defense community where it has been very successful.

DDS is a platform-independent technology that can run on lots of different platforms including servers, desktops, mobile platforms, embedded systems, sensors and even web browsers. It supports low-latency, predictable, secure, fault-tolerant and interoperable communications. The DDS automatic discovery features allow applications to easily find each other regardless of location. This feature makes it an excellent technology for implementing an edge network using Cloudlets. It also provides a decentralized architecture with support for peer-to-peer communications. Again, this is an important feature for supporting network centric edge networks.

DDS has been recommended by governments worldwide and is a mandated technology on many military projects. It is also an important enabling technology for organizations such as Eurocontrol, which manages air traffic control across Europe, and the Open Source Robotics Foundation, which is recommending the use of DDS in its ROS 2.0 specification.

5. Vortex DDS the Proven DDS Solution for Network Centric Systems

ADLINK has been supplying its advanced middleware platform technologies to the defense and aerospace community for more than 20 years. ADLINK's products are used by many of the largest defense companies, supporting many different application use cases.

Vortex DDS is ADLINK's real-time data sharing platform for mission-critical and Industrial IoT systems, which is based on the DDS standard. Vortex DDS enables real-time data sharing across a range of platform (mobile, severs, web, embedded, sensor) and network configurations including native support for cloud and fog/edge computing architectures.

In addition to the aerospace and defense markets, Vortex DDS is used in a wide range of commercial markets including large-scale transportation systems, smart energy and utilities, industrial automation and connected healthcare systems.

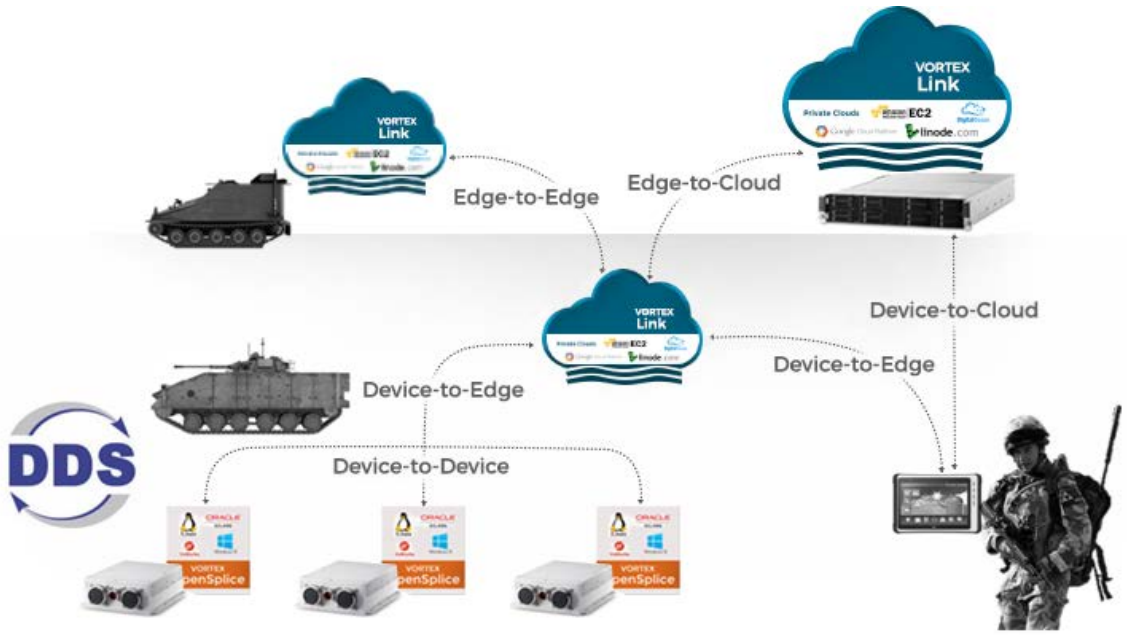

Figure 7 – Battlefield Data Dissemination Enabled by Vortex DDS

Vortex DDS is used on many defense-related projects across a range of application areas such as radar processors, vetronic systems, autonomous systems (UAV, USV, UUV, etc.), naval combat management systems, land systems and other next-generation network centric systems.

Vortex DDS is unique in that it optimally addresses the data connectivity needs of both peer-to-peer, real-time tactical edge networks and data connectivity over a wide area network with a cloud-based data center. Vortex DDS provides a suite of technologies based on the DDS standard that can be used to enable end-to-end data connectivity in a network centric system. It consists of interoperable implementations that can be used to support the different types of device platforms found in enterprise and tactical edge environments.

Vortex DDS provides core capabilities, such as automatic discovery, time and space decoupling, peer-to-peer communications and reliable information exchanges independent of the underlying network that make it suitable for enabling ad-hoc tactical edge networks using Cloudlets. For example, soldiers on the battlefield can communicate on their mobile equipment with Cloudlet servers via Vortex DDS apps on their personal devices.

Where a shared operational picture and mission planning is required wide area connectivity and data sharing can be achieved by sharing data securely from the edge network over the wide area network using Vortex DDS.

6. Summary

There is an increasing trend to leverage cloud computing in network centric military systems. This is in part being driven by the latest defense initiatives such as the DoD's third offset strategy focused on investing heavily in mobile, autonomous systems, miniaturization, robotics, big data and COTS technologies.

However, cloud computing has a number of limitations for tactical edge systems where connectivity to the core network is intermittent or not possible, there is a large volume of data to be processed, network bandwidth may be limited and the network latency from the edge to the cloud is too high.

Tactical Cloudlets are a means to make cloud services and processing available to mobile users by offloading computation to servers deployed on platforms closer to the users. Cloudlets leverage capabilities such as automatic discovery and VM based provisioning, combined with peer-to-peer communications.

From the beginning the DDS standard was designed to support the requirements of the GIG and network centric systems. DDS is a real-time, data-centric peer-to-peer protocol that is well suited to support a tactical edge architecture leveraging a network of Cloudlets.

Vortex DDS is the most effective and proven DDS solution stack for next generation network centric military systems and provides native support for cloud and edge/fog/Cloudlet computing.

Web: www.adlinktech.com

Email: ist_info@adlinktech.com

Notices