CONTENT BANDWIDTH MANAGEMENT (CBM) ADAPTIVE NETWORK SERVICES

THE CHALLENGE

Modern tactical networks are increasingly under strain due to the growth of high quality sensors, significant Command and Control (C2) track data and coordination content generated by Voice over IP (VoIP), Video Teleconferencing (VTC) and Chat systems. The acquisition and deployment of these content producers far outpaces the parallel improvements in the transmission systems that carry the data between the producers and their consumers. The expeditionary nature of the United States Marine Corps (USMC) further aggravates this imbalance because it forces the Marines to rely on Disadvantaged, Intermittent, Low-Bandwidth (DIL) networks that are often served via Beyond Line of Sight (BLOS), satellite transmissions systems. The Marines have good network Situational Awareness (SA) data but they need a cost-effective, reliable way to ensure delivery of the content across their DIL networks.

THE STRATEGY

In 2009, Headquarters Marine Corps Command, Control, Communications and Computers (HQMC C4) tasked CSCI to investigate automated solutions that could monitor network conditions, receive various policy inputs and combine this network health information with governing policy to perform positive control over the transmitted content. CSCI chose a Service Oriented Architecture (SOA)-based approach that would facilitate rapid prototyping and independent evolution between the various CBM Adaptive Network Services (ANS) components. The components included: a Content Treatment Service (CTS) that managed Full Motion Video (FMV), a Content Registration Service (CRS) to provide information on offerings and SA on CTS locations and status, a Simple Network Management Protocol (SNMP)-based Network Interrogation Service (NIS) to observe the network, a representative Identity Management Service (IDMS) to correlate consumers with their logical location on the network, a Governance Service (GvS) to incorporate policy inputs and conduct load-balancing between content and a Network Visualization Service (NVS) that converted network health information into Cursor on Target (CoT) messages that could be geo-registered and monitored via organic USMC Common Operating Picture (COP) software hosted on Windows laptops and Android tablets. These lightweight, SOA-based services were hosted on CentOS (Linux) virtual machines (VMs) and physical laptops in a distributed mesh across tactical USMC networks.

CSCI began conducting evaluations of CBM ANS at the Marine Corps Network Efficiency Lab (MCNEL) at the Marine Corps Tactical Systems Support Activity (MCTSSA) command at Camp Pendleton, CA. Subsequently, CSCI obtained Authority to Operate (ATO) certifications for a CBM Reference Implementation (RI) so it could be tested, evolved and tested again during several Weapons and Tactics Instructor (WTI) courses from April 2012 (WTI 2-12) through April 2017 (WTI 2-17) on WTI's live, Tactical Secret Internet Protocol Router Network. These tactical demonstrations included simulated as well as live FMV from Unmanned Aerial Vehicle (UAV) assets, monitoring the utilization and health of various LOS and BLOS transmissions systems and receiving input from Information Management Officer (IMO) tools that enabled the CBM ANS infrastructure to maintain positive control over the content and its effects on the tactical network.

THE RESULTS

CSCI's CBM ANS RI demonstrated tangible improvements to MCTSSA and with Marine Wing Communication Squadrons 28 and 38 supporting WTI. In contrast to the USMC's current, unmanaged approach, network overutilization was prevented by automated control of the CTS. The CTS even terminated its FMV transmission when degraded network conditions prevented positive control by the GvS – enabling the network to recover and network administrators to regain access to their network resources. By carefully sizing the FMV, usable SA was provided to consumers – even under DIL conditions. Automatic load-balancing by the GvS ensured that CBM-controlled FMV properly shared available network resources and all content was delivered in parallel. The result: delivery of live, geo-registered network health information validated by MWCS network monitors was a significant improvement over their current, non-granular and non-geo-registered solutions.