Proceedings of the 2006 Winter Simulation Conference
L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto, eds.

CONCEPTUAL LINKING OF FCS C4ISR SYSTEMS PERFORMANCE TO INFORMATION QUALITY AND FORCE EFFECTIVENESS USING THE CASTFOREM HIGH RESOLUTION COMBAT MODEL

H. Todd Minners

TRADOC Analysis Center - WSMR
White Sands Missile Range
White Sands, NM 88002, U.S.A.

Douglas C. Mackey

TRADOC Analysis Center - WSMR
White Sands Missile Range
White Sands, NM 88002, U.S.A.

ABSTRACT

TRAC WSMR implemented several enhancements to the CASTFOREM high resolution combat model to enable analysis in support of DoD FCS Program acquisition decisions. The overall framework for FY06 FCS network analysis centers on the inherent linkage between the performance of components of the FCS C4ISR network and FCS force level outcomes. This framework suggests that the performance of the supporting C4ISR systems influences the quality of information available to the decision maker. That information drives the level of situation awareness that the decision maker achieves and the quality of the decisions published. Those decisions in turn enable the effective application of the elements of combat power and drive the observed force level outcomes.

This paper describes major M&S enhancements and a methodology to assess the above linkage. We discuss CASTFOREM communications modeling and information flows, platform situational awareness (SA) databases and Common Operational Picture (COP), decision-making logic, and fusion algorithms.

1 INTRODUCTION

The Combined Arms and Support Task Force Evaluation Model (CASTFOREM) is a high-resolution, force-on-force, stochastic constructive model of a combined arms conflict. It was developed by the United States Army Training and Doctrine Command (TRADOC) Analysis Center-White Sands Missile Range (TRAC-WSMR). Scenarios are variable in size but typically are at Brigade or below. Echelons above Brigade are played to the extent that they support the Brigade being simulated, to include Joint assets.

CASTFOREM models all types of direct fire, crew-served ground weapons systems; helicopters; dismounted infantry; conventional artillery; engineering operations; combat service support; communications; maneuver with capability of dynamic route selection; detailed search and acquisition; realistic battlefield obscurants; and digitized terrain.

Each organizational entity possesses a singular intelligence database this is updated by the procurement of information via the communication network or directly by its own organic sensors. Measurement errors at the sensor level or delays and failures in the exchange of information over the communications network result in each entity's intelligence database to be a perception of ground truth and not ground truth itself.

Each organizational entity is provided a knowledge base which allows that entity to act and react according to doctrine. The knowledge base is represented as a set of production rules in decision tables. These rules are typically determined by the military schools or subject matter experts. Depending on the entity echelon of command, the knowledge base may be very complex or simple.

Up until 2001, CASTFOREM was focused on the simulation of legacy military systems. In 2001, CASTFOREM began a series of substantial upgrades to enable it to simulate the systems that comprise FCS. The upgrades continue to evolve as the FCS program does.

These upgrades include the implementation of algorithms to more precisely simulate the communications network, the distribution of situational awareness (SA) databases, and the applications that use the database. The primary application of interest has been networked fires.

2 MODELING THE FCS COMMUNICATIONS NETWORK

The FCS communications network currently modeled in CASTFOREM includes the following waveforms: wideband networking waveform (WNW), soldier radio waveform (SRW), network data link (NDL), and Ka SATCOM. (Legacy waveforms for EPLRS and SINCGARS were implemented in the 1990s.)

Within each waveform, the modeling starts with establishing the matrix of node-to-node physical connectivity. A link is open (i.e., physical connectivity exists) if the actual

path loss between the nodes is less than the radio's link path margin. Otherwise, it is closed. Once the node-to-node physical connectivity is determined, the nodes are configured into the appropriate network node groupings.

The WNW network nodes are grouped using a regions-based topology. A region is an maximally connected set of nodes, with a node designated as the Region Access Points (RAP). For a message to ingress or egress from a region to another region, the RAP is used as the gateway (C4ISR IPT 2005).

The SRW network nodes are grouped using an islands based topology. For islands-based subnets there is a two-tier hierarchy with local communications within lower-tier islands and with extended communications range via an upper-tier island (C4ISR IPT 2005).

The NDL waveform is currently used for the communications link from unmanned aerial vehicles (UAVs) and reconnaissance helicopters with sensor feeds to their ground stations. It is played as a simple 1-on-1 link.

The Ka SATCOM waveform is used to simulate the future War-fighter Information Network–Tactical (WIN-T).

In the CASTFOREM model for a BCT-sized scenario, the computationally-intensive network reconfiguration process occurs every 30 minutes to balance the need to capture dynamic changes to the network node connectivity and simulation run times. For smaller scenarios, this NxN matrix network reconfiguration can be set to more frequent values (Brooks 2004).

2.1 Message Flow

Given a message to be sent by a node to another node within a waveform, a route is selected based on the open shortest path first (OSPF) protocol. Each open link is assigned an a priori cost weight and the Dijkstra algorithm uses those weights to determine the least cost path. If the message is sent unicast, then only one route is computed. If the message is sent multicast, then all routes are computed explicitly.

Once the route is determined, performance curves are used to lookup and provide a completion rate and time delay, by hop and by packet, as a function of the waveform, data rate, network utilization, message priority, transport type (e.g., reliable or unreliable), and the number of active radio frequency (RF) neighbors. The performance curves are produced using the OPNET model by CERDEC/MITRE, validated by AMSAA and provided to TRAC for use in CASTFOREM for each type of communications waveform (Brooks 2004).

In CASTFOREM, the user can define the priority, transport type (reliable or unreliable), and bandwidth reserved for that type of message. This message priority and associated bandwidth reservation scheme provide a rudimentary implementation of the FCS concept for Quality of Service (QoS) until more specific data becomes available.

Obviously, these message types are a simple subset of the traffic load in the 'real world'. To capture a more realistic loading of the network, TRAC WSMR, in collaboration with SIGCEN and MITRE, has implemented an implicit traffic flow model in CASTFOREM. This method cyclically instantiates background flows of data and voice messages that are derived from the full set of information exchange requirements (IERs) provided by BCBL-G and that are NOT explicitly played internal to CASTFOREM. They are called 'flows' because they persist for the duration of the cyclical interval. So, in computing network utilization to determine completion rate and time delay at any given hop in a route, the background or implicit flow is added to the explicit traffic generated internal to CASTFOREM (Brooks 2004).

If the sender and receiver are on separate waveforms, the message will be routed using established protocols. For example, if a soldier using SRW needs to communicate to a vehicle on WNW, the message is currently routed through his carrier vehicle which has both waveforms and can act as a gateway.

2.2 Electronic Warfare

CASTFOREM models Electronic Warfare as either communications jamming or GPS jamming. For communications jamming, the jammer units are portrayed as individual vehicles or systems with appropriate maneuver and jammer on-off-cycle tactics. Currently, Blue reaction to and countermeasures for Threat jamming are not played. The jamming algorithm algorithm effects a change in the physical network connectivity matrix which has an impact on waveform topologies as long as it's in use. It first checks if a receiver is within the jammer footprint, and then calculates the signal to jammer ratio, based on the effective radiated power of the transmitter and jammer and the power of the signal received and jammer. For each node-to-node pair, the potential sender node's signal power is compared to the jammer power received at the potential receiver node. This signal-to-jam ratio is then compared to a given threshold to see if the physical link is severed and if so, the network connectivity matrix is modified accordingly. Messages is not completed due to jamming are recorded as jammed in the CASTFOREM network performance file. CASTFOREM represents GPS jamming as user-defined on/off jamming times, and the effects are applied across the entire battlefield.

3 MODELING THE COP AND THE DISTRIBUTION OF SA DATABASES

The COP is used as the basis for implementing the FCS networked fires process to include target selection and frat-

ricide checks. CASTFOREM can establish and maintain two distinct SA databases at any tactical platform such as a C2V , commander's vehicle or individual soldier: friendly SA database and threat SA database.

3.1 Maintenance of Friendly SA Databases

The friendly SA database is typically updated via a 'heartbeat' reporting of all friendly entities to the collection entities. The information received is time tagged, has the explicit addressee identifier, the entity's current position estimate that includes GPS location errors, its platform's current damage profile, fuel level, and ammo levels.

Upon the receipt of a friendly SA report the database is updated by simply replacing the old data with the new. The maintenance of this database enables the calculation of Blue information metrics such as information correctness, completeness and accuracy (these are described more later).

3.2 Maintenance of Threat SA Databases

The information received is time tagged, has a track id assigned, has an estimated x and y position and associated target location error based on the acquiring sensor (as an independent sample, as opposed to previously fused), a BDA, and an acquisition discrimination level.

Upon receipt of a threat SPOT report, the CASTFOREM level I fusion algorithm is used to determine if the incoming track associates with any existing tracks and, if so, the x and y position estimates are fused.

Association is based on gating and sequential nearest neighbor correlation using the Mahalanobis metric (Chi-squared statistic) (Hall 1992). There is also an option to play perfect association if needed for analysis. When using CASTFOREM to compare FCS operations to legacy operations, typically we use perfect association to 'maintain a level playing field', since legacy association algorithms are typically human in the loop and have not been quantified for use in combat models.

Upon association, position estimates are fused using a Kalman Filter which uses the sensor target location errors to maintain a covariance matrix on the position estimate. Also upon association, fusion of the BDA and acquisition levels is performed as a simple 'keep the highest level' heuristic.

3.3 Distribution of Friendly SA Databases

Currently friendly SA databases are 'pushed' periodically from company to battalion commanders, from battalion commanders to the brigade commander, and across to other battalion commanders, and on down to their company commanders (C4ISR IPT 2005). To conserve bandwidth, only those friendly positions for which there was an update will be pushed out across the network.

3.4 Distribution of Threat SA Databases

Currently threat SA databases are requested periodically by the brigade commander from the echelons above brigade commander. In turn, battalion commanders within the brigade will periodically request a download of the brigade threat SA database. As for the Blue SA database transfers, only those tracks that have been updated since the last download are sent to save on bandwidth.

Upon receipt of a threat SA database update, the fusion process is rudimentary. The statistical association algorithm using the Mahalanobis metric requires that the incoming position estimate be an independent sensor sample, but this incoming position estimate may be the result of previously fused position reports. Hence, association consists of simply trying to find an existing track with same track id as that provided. (Hall 1992)

If the new track does not 'associate', it is instantiated as a new track. This could produce redundant tracks. If the new track does 'associate', we also need to prevent the Kalman Filter from mathematically fusing already fused data (double fusion problem). To prevent this, we simply compare the variance (as provided by Kalman Filter) of the incoming position estimate to the existing track's variance and retain the position estimate of smaller variance. Fusion of BDA and acquisition level is, once again,'keep the highest level' heuristic.

4 MODELING NETWORKED FIRES

The networked fires application uses the friendly and threat SA databases of the FCS COP. Typically brigade and battalion commanders, upon receipt of a threat SA database update, will enter the networked fires application implemented in CASTFOREM. It consists of using a set of production rules, provided as a knowledge base as a function of commander and battle phase, to sort through the set of current threat tracks, and do a pattern recognition scheme as a rudimentary level II and III fusion algorithm to first determine situational assessment and then to determine the threat assessment. This is intended to simulate the automated and human-in-the-loop processes that produce the desired prioritized list of targets to be serviced.

For each target in priority order, the fire unit that can physically accept and fire the highest priority round is then sent the mission. This can be viewed as a discreet gradient search of a feasible region to find the 'optimal' solution of a non linear optimization problem.

Upon allocation of a munition to a target track, the track is marked as 'awaiting BDA'. Upon receipt of a BDA report, the target status is updated and the target will be disposed of accordingly.

5 NEW METRICS TO QUANTIFY INFORMATION QUALITY

Starting with the FBCB2 AoA, CASTFOREM has been modified and improved continuously for use in assessing the value of tactical information available to key decision makers and the impact of the quality of this information on decision making and ultimately force outcomes. To support this type of analysis, TRAC has developed metrics to measure network performance and information quality over time and by phase of a tactical operation in order to capture the impacts network performance during more and less stressful times in the battle. For example, by evaluating message completion rates (MCR) (a network metric) and force OPTEMPO (a force effectiveness metric) over time, it is often possible to assess the impact of network performance on force effectiveness. Similarly, an assessment over time of kills by Joint assets (a force effectiveness metric) and currency of Threat reports in a Blue commander's COP (a network metric) will enable discovery of any correlation between information quality and Joint lethality.

Of the six criteria for information quality described in Field Manual (FM) 6-0, CASTFOREM can currently measure Currency of Threat/Blue Information, Correctness of Threat/Blue Information, and Percent of Known Threat/Blue Entities.

The above measures can be calculated for any entity but are typically assessed for the BCT commander, battalion commanders, and selected company commanders. The Currency of Threat/Blue Information measure is a measure of how current the Threat/Blue information is on the selected commander's COP.

6 CONCLUSION AND THE WAY AHEAD

TRAC WSMR continues to improve the CASTFOREM high-resolution closed form combat model to provide enhanced analytical capability in the areas of information quality, network-centric battle command and information impact of force effectiveness. Recent improvements to support analysis of FCS networks have enabled new analytical insights and the integration of CASTFOREM-derived analysis with performance and engineering model outputs has increased the relevance and credibility of analysis in support of DoD and DA acquisition decisions. Much work remains to expand model capabilities to assess network reliability, Blue vs. Threat information quality (information overmatch), and the impacts of other types of network degradation such as IP intrusion and fragmented packets on information quality and force effectiveness.

REFERENCES

Brooks, Charles. 2004. Modeling C4ISR for the Future Combat Systems (FCS) System Development and Demonstration (SDD), version 2.3. Available via MITRE.

Hall, David L. 1992. Mathematical Techniques in Multisensor Data Fusion. Available via Artech House, Boston.

C4ISR IPT. 2005.(PM UA NSI & LSI) C4ISR Network Assumptions. White Paper. Version 8.0, 6 September 2005.

AUTHOR BIOGRAPHIES

H. TODD MINNERS is a US Army LTC and Study Director for Army Integrated Network Analysis at the US Army TRADOC Analysis Center, White Sands Missile Range, NM. As a combat operations analyst, he has experience with the CASTFOREM model for high-resolution network analysis in the FBCB2 AoA and various FCS network configuration analyses over the last 4 years.

DOUGLAS C. MACKEY is chief programmer for CASTFOREM at US Army TRADOC Analysis Center at White Sands, New Mexico. He has worked on CASTFOREM since 1979. He holds a M.S. in Mathematics and a M.S. in Statistics from Michigan State University.