Toward Linking Information Assurance and Air and Missile Defense Mission Metrics

The Johns Hopkins University Applied Physics Laboratory
Laurel, MD
Email: amy.castner@jhuapl.edu

Abstract—With the growing reliance on net-centric warfare, understanding the effect of information operations (IO) on the overall mission becomes increasingly important. Our research seeks to develop metrics that provide insight into the mission-level effect of IO. We approach this goal by proposing comprehensive mission success metrics that provide a vehicle to analyze correlation with proposed information metrics. A quantitative analysis of relationships among information and mission metrics yields an ability to predict mission effect based on activity in the information space. This in turn may drive the derivation of operational requirements and the development of technology and strategy to better assure the mission. This paper presents initial progress toward identifying promising links between mission-level metrics and information metrics, as well as insights into potential applications, such as a combat system that adapts to information degradation.

Index Terms—Information Assurance, Air and Missile Defense, Metrics, Mission Assurance

I. MOTIVATION

As the defense community continues to shift toward net-centric warfare, it becomes increasingly important to understand the effect of information operations (IO) on the overall mission. IO uses tactics such as electronic warfare and computer network operations to influence, disrupt, corrupt, or usurp adversarial human and automated decision making, while protecting our own [1]. Collaboration among units within a net-centric force yields improved performance, but requires an increased reliance on communication networks and information exchange. During network attacks, this reliance may present an Achilles heel.

Our research seeks to build a quantitative understanding of the relationships among IO actions and mission effects. Traditional risk assessment analyzes attack impact and likelihood of occurrence [2][3][4][5], but it remains difficult to quantify mission-level impact. Several recent research endeavors have sought to comprehend the relationship between information attack and mission impact [6][7][8][9][10]. Recently, we investigated methods to quantify the impact of IO on Air and Missile Defense (AMD) force-level mission performance [11]. This research developed a simulation-based approach to measure the impact of information attacks on AMD performance. We also made initial progress toward identifying mid-level metrics that could link events in the information space to mission-level effects. Such analysis yields an ability to predict the effects of information attacks and identify requirements for mitigation. Decision makers can use these analysis techniques to drive information assurance (IA) investments and requirements based on an understanding of how proposed mitigations will affect mission performance.

In this paper, we focus on metric development and its applications. We propose improvements to previously identified mission success metrics and develop additional concepts for information metrics that link IO and mission effect. We discuss our quantitative analysis approach and simulation environment. We also introduce potential applications for analysis results, including the derivation of quantitative operational IA requirements and support for tactical decision-making within the force.

II. BACKGROUND

We begin by defining the AMD scenario considered in our analysis. This scenario is based on Navy combatants in a Tactical Situation (TACSIT) from the Major Combat Operations 3 scenario, which is outlined in the Defense Planning Guidance document. The scenario consists of a blue force that engages a red force consisting of airborne threats. The blue force seeks to provide Area Anti-Air Warfare Defense to a set of protected assets.

The blue force is composed of a number of independent agents that coordinate actions to engage threats and minimize damage to protected assets. There are a variety of options for threat engagement schemes; here we focus on a distributed auction algorithm that allows each agent to bid on engagements. Coordination occurs by a process in which each agent independently evaluates the relative difficulty or cost of engaging a particular threat and shares those cost estimates with its peers. Given a shared cost map, which defines engagement difficulty for each agent-threat pair, each agent uses the same algorithm to optimally allocate itself and its peers to engage the known threats. Without effective coordination, engagements are redundant or inadequate, resulting in decreased mission success.

To date, our research has considered the effect of denying Command and Control (C2) information (i.e., auction bids), changing Planning Network data (i.e., defended asset priorities), and injecting false Air Picture Network data (i.e., by creating false tracks). Here, we focus solely on denial of C2 information required to execute engagement coordination in an auction-based scheme.
Figure 1 shows the engagement coordination process for a simple scenario with two agents. By nature, the distributed algorithm assumes that each agent will generate the same output given the same input. Thus, a notional information attack may degrade mission performance by denying or changing bids exchanged among agents in order to create uncommon cost maps. Significant differences in cost maps across the force introduce confusion that causes the agents to make different engagement decisions, potentially resulting in decreased mission performance.

**III. Metrics**

Our previous work demonstrated that information attacks could have an effect on mission-level outcome. Here, we seek to develop metrics that enable quantitative analysis of events in the information space and their mission-level effects. This section refines our mission success metrics and presents concepts for information metrics that are particularly insightful for the AMD scenario under study. We also discuss our approach to correlation analysis that will enable the recognition of cause-and-effect relationships among these metrics. Ultimately, we seek to use this analysis technique to identify key relationships between IO actions and mission effects.

**A. Mission Metrics**

The air and missile defense (AMD) mission is to protect friendly assets from airborne threats, including enemy aircraft and missiles. As such, we measure mission effectiveness in terms of damage sustained by the protected assets. Our initial work measured mission success using a pair of metrics: (1) Leakers (i.e., the number of threats not destroyed), and (2) Inventory Expended (i.e., the number of interceptors fired during engagement). We have recently refined these measures to better account for the underlying scenario and developed techniques to aggregate a holistic mission success measure.

1) **Kill Ratio:** Our previous work used the number of leakers as the chief measure of AMD mission performance. Low leaker metrics indicated a successful mission. The leaker metric is insightful when working with a constant number of threats; however, it is difficult to compare leakers across scenarios with different numbers of threats. For example, a single leaker in a scenario with 100 threats is very different than a single leaker in a scenario with 10 threats.

We developed a new metric called Kill Ratio in an effort to normalize our results. Kill Ratio is defined as:

\[ R_K = \frac{N_K}{N_T}. \]

where \( N_K \) is the number of threats killed and \( N_T \) is the total number of threats. Kill Ratio ranges from 0 to 1, with higher values indicating increased mission success. It may not always be possible to reach \( R_K = 1 \) due to inventory constraints.

2) **Inventory Efficiency:** Our previous work also considered inventory expended as a secondary measure of mission success. High inventory usage suggested inefficient engagement coordination and decreased mission effectiveness. Similarly, we developed a new metric that seeks to quantify inventory efficiency to enable comparison across scenarios. We define the Inventory Efficiency, \( E_I \), metric:

\[ E_I = \frac{N_K}{X_I}. \]

where \( X_I \) is the total inventory expended. Like the Kill Ratio, the Inventory Efficiency metric normalizes our inventory measure by considering the number of kills achieved with expended inventory. Inventory Efficiency ranges from 0 to 1, with 1 indicating optimal inventory usage.

3) **Holistic Mission Metrics:** Kill Ratio and Inventory Efficiency measure the effectiveness of different aspects of mission success (i.e., destruction of all threats and optimal use of inventory, respectively). We may aggregate such diverse mission success metrics by defining a holistic mission effectiveness metric. Metric aggregation requires addressing subjective considerations such as the relative importance of various aspects of the mission. For example, is it more costly to allow an additional leaker or expend an additional missile? Here, we propose a weighted sum to allow for metric aggregation. Mission Effectiveness, \( E_M \), is defined as follows:

\[ E_M = w_K \cdot R_K + w_E \cdot E_I, \]

where \( w_K + w_E = 1 \). The selection of weights is subjective and represents the relative importance of the individual mission success metrics. In this case, it quantifies the relative importance of a leaker compared to the depletion of additional inventory. Weight selection must also consider correlation among individual factors.

This concept may be expanded to include additional mission success measures as they are identified. For example, an aggregate mission effectiveness measure may also need to consider leaker impact by quantifying the number and relative importance of destroyed assets. Such an addition would account for differences in the relative impact of leakers against various targets.

**B. Information Metrics**

By tracking Kill Ratio and Inventory Efficiency, we are able to consistently gauge AMD performance in a variety of situations. In particular, we are interested in mission performance during an attack on agent communications, which in turn interferes with engagement coordination. We seek
to measure the extent to which coordination fouling affects AMD mission execution. In support of this goal, we have developed three families of information metrics that reflect the effectiveness of information sharing and decision coordination.

We compare information metrics and mission performance metrics to identify information metrics that exhibit useful correlation and, as such, provide insight for strategic investment in communication robustness or tactical decision adjustments to account for detected coordination errors.

The first family of information metrics addresses commonality and entropy of shared information. These metrics measure the extent to which each agent is acting in accordance with the same cost map. Each agent may have a slightly different map since agents do not always communicate small changes in their cost estimates of engaging threats. However, large differences can cause inadequate or redundant threat coverage. We seek to measure the extent of differences in agent cost maps (information entropy), the extent to which agents have the “correct” maps (information commonality), and the rate at which the information commonality changes.

The second family of information metrics addresses decision commonality and entropy. These metrics measure the extent to which engagement assignments are common across agents (decision entropy), the extent to which agents have the “correct” engagement assignment (decision commonality), and the rate at which the decision commonality changes.

The third family of information metrics we consider are graph-based. In each simulation, we build a communication graph that dictates available communication channels among each of the agent pairs during an attack. We identify four groups of agents: (1) those that cannot communicate (i.e., isolates), (2) those that can both send and receive (unaffected by the attack), (3) those that can send only, and (4) those that can receive only. The communication graph is shown in Figure 2. In the case where every agent is affected by an attack, every node is an isolate and no arcs are present. In the case of full communication, every node can both send and receive and every arc is present. We calculate several graph-based metrics, including the proportion of agents in each of the above four groups, degree centrality [12], and degree measures (e.g., average degree, in-degree and out-degree). Supporting graph theory is presented in [13]. An attack on communications directly affects the structure of this graph, and thus the values of these metrics.

Our identification these factors as key metrics is closely tied to the AMD scenario under study. The auction algorithm relies heavily on information exchange and distributed algorithms reaching the same conclusions given the same initial data. It is likely that further analysis of additional scenarios will yield insight into additional metrics that affect mission success. For example, an attack that compromises bid integrity can lead to common but inaccurate cost maps. This in turn may cause the distributed algorithms to generate common bad engagement decisions that degrade mission performance. Thus, common decisions cannot guarantee good mission performance; however, uncommon decisions will likely lead to some level of performance degradation.

C. Linking Information Metrics and Mission Effectiveness

Our research seeks to identify fundamental correlations between information metrics and mission-level effects. As a result, our methodology is based on quantitative analysis of simulation results for AMD scenarios of interest. We use two separate simulation environments: (1) APL Coordinated Engagement Simulation (ACES), and (2) a lightweight MATLAB model that isolates engagement coordination for close study. ACES is a force-on-force engagement-level Monte-Carlo AMD simulation that has been used to develop and analyze advanced engagement coordination algorithms for a Joint Integrated Air Defense Environment [14]. Here, we scope our analysis to the lightweight MATLAB model in order to study correlation between commonality and mission metrics without potential interference from other factors. The MATLAB model also provides significantly faster runtimes (e.g., 15 seconds instead of 1 hour for a 7-agent simulation).

1) Analysis Approach: Our MATLAB model executes Monte-Carlo simulations in which communication among agents and engagement coordination decisions occur in a manner similar to the original ACES simulation. In this case, engagement cost for each agent-threat combination is randomly generated and modified throughout the simulation. Agents evaluate target options and their knowledge of other agents’ intentions at each time step and update their engagement plans accordingly. The simulation calculates the mission and information metrics described in Sections III-A and III-B. The user chooses the number of agents, the number of threats (which is assumed to be less than or equal to the number of agents), the information attack start and end times, which agents can send and/or receive during the attack, and whether the attack is continuous or intermittent. To further constrain the problem, we assume that every agent has only one missile to use.

Our analysis seeks to identify information metrics that are able to predict mission success measures (e.g., Kill Ratio and Inventory Efficiency). We perform exploratory analysis and use our results to build linear regression models that rely on
information metrics to predict mission metrics. It is desirable to create a “simple” model (i.e., a model with as few variables as possible while still being robust and useful). Simplicity helps us avoid overfitting the data. Additionally, we assume that in a real-life scenario, only a few information metrics may be calculated online. Thus, although several information variables may have predictive power when it comes to mission metrics, including more in our model may have limited benefit.

At the mission level, our analysis focuses on Kill Ratio and Inventory Efficiency in two different scenarios. The first scenario subjects a subset of the force to a continuous denial of service attack that lasts for the entire simulation (100 time steps). In the second scenario, the denial of service attack is intermittent throughout the duration of the simulation. Each time an affected agent tries to communicate during the attack, there is a 25% probability they will succeed. In both scenarios, the set of agents that have full communication, send ability only, receive ability only, and no communication varies. Given $n$ agents, each partition of $n$ into four or fewer parts is considered and five Monte-Carlo simulation runs are performed with that communication structure.

2) Results: Here, we examine the ability of several information and scenario-based metrics to predict mission effectiveness by building statistically significant linear regression models for Kill Ratio and Inventory Efficiency. For background on regression, see [15]. Not surprisingly, the variable with the strongest influence on both Kill Ratio and Inventory Efficiency is the Threat to Agent Ratio, $R_{TA}$, defined as:

$$R_{TA} = \frac{N_{A}}{N_{A}}$$

where $N_{A}$ is the number of agents. This is certainly an intuitive result. If the Threat to Agent Ratio is low, then there are many agents covering just a few threats. In the case of poor communication, every agent will assume they need to cover at least one of those threats. Thus, most threats are bound to be covered by at least one agent, and probably by multiple agents. If the Threat to Agent Ratio is high, then it is more critical that the agents work together to engage the threats and use their inventory efficiently.

As introduced in Section III-B, we consider three classes of information metrics: information commonality, decision commonality, and graph-based. We begin by examining the Rate of Change of Information Commonality, which has a strong influence on Kill Ratio. At every simulated time step, information commonality of a given agent-threat pair $(a, j)$ is equal to the number of agents that agree with agent $a$ about how much it would cost for agent $a$ to engage threat $j$. At time step $t$, we call this value $\text{comm}(a, j, t)$. The rate of change of information commonality of a given agent-threat pair $(a, j)$ is the difference of information commonality from one step to the next. We define this to be:

$$\Delta_{c}(a, j, t) = \text{comm}(a, j, t) - \text{comm}(a, j, t-1), \quad t \geq 2.$$  

The Rate of Change of Information Commonality metric aggregates these rates over all jobs, agents, and time steps and normalizes the result to allow comparison among scenarios with different parameters (e.g., number of agents). If $T$ is the time of the last threat of the simulation, $J(t)$ is the number of threats remaining in the simulation at time $t$, and $J$ is the set of remaining threats, then this metric, $R_{IC}$, is defined as:

$$R_{IC} = \frac{\sum_{t=2}^{T} \sum_{a=1}^{N_{A}} \sum_{j \in J} \frac{\Delta_{c}(a, j, t)}{N_{A} \cdot J(t) \cdot (N_{A} - 1)}}{T - 1}.$$  

A positive value of the Rate of Change metric indicates that, on average, information commonality is increasing over time. Increasing commonality is expected to improve the decisions made by agents, which is evident in an increase in Kill Ratio. This relationship is shown in Figure 3 for data with Threat to Agent Ratio in $(0.50, 0.75)$.

Information Entropy also has a strong influence on Kill Ratio. For an agent, job, time step triple, $(a, j, t)$, we define $\text{Ent}(a, j, t)$ to be the entropy of the cost value beliefs over all agents for that agent, job pair at time $t$. If $I$ is the number of distinct beliefs about the cost of agent $a$ to engage threat $j$ at time $t$, then define $p_{i}$ to be the proportion of agents that hold belief $i$ for $i = 1, \ldots, I$. Then,

$$\text{Ent}(a, j, t) = -\sum_{i=1}^{I} p_{i} \ln p_{i}.$$  

The Information Entropy metric aggregates this value over all agents, jobs, and time steps and then normalizes the result to allow comparison. Using the same notation as above, we obtain $\text{Ent}_{I}$.

$$\text{Ent}_{I} = \frac{\sum_{i=1}^{I} \sum_{j \in J} \sum_{a=1}^{N_{A}} \text{Ent}(a, j, t) \cdot \frac{1}{T}}{T}.$$  

Information Entropy is more a measure of agreement among agents, rather than agreement with the agent in question.
and less than 0.25. The data points indicate that Inventory Efficiency increases as the Normalized Average Degree increases.

The final linear model we found for Kill Ratio is

$$R_K = 2.15 - 0.72R_{TA} + 0.10N_A - 0.67N_A^{1/2} + 4.42R_{IC} - 0.09Ent_I - 27.73R_{IC} \cdot Ent_I.$$  

The adjusted R-squared value is 0.48, the standard error is 0.15, and the p-value is near 0. Including additional variables does not significantly improve the R-squared value. We find a similar model for the intermittent attack, although that model does not significantly improve the R-squared value. We find a significant difference again in the adjusted R-squared value to 0.13. Inventory Efficiency clearly suffers greatly from the additional noise produced from intermittent attack.

IV. APPLICATIONS

A detailed understanding of the relationships among information metrics and mission effects enables strategic improvements to mission execution. We propose to use our analysis results to identify quantitative operational requirements for information and network assurance and to provide insight into technology and procedures that can better assure the mission.

A. Derivation of Requirements

It is unlikely that we will ever be able to completely prevent information attacks. Realistically, we should seek to minimize the effect of attacks on the mission by building technologies and procedures that assure information and network resilience. Our analysis seeks to enable the derivation of operational requirements for information and network assurance that will in turn minimize the effect of attacks on mission success. To demonstrate this concept, we are conducting a series of experiments in our MATLAB model.

Our goal in this analysis is to determine temporal and spatial requirements to assure sufficient information sharing among agents within the model. Thus, we introduce a simple physical model that calculates engagement cost by squaring the distance from agent to threat. Distances between agents and threats vary according to a simple model throughout the simulation. We define synchronization as a condition in which a single agent engages each threat. Desynchronization occurs when a threat is not engaged or when it is engaged by more than one agent. In order to develop an understanding of temporal and spatial requirements for effective engagement, we study the model under a variety of operating conditions. We vary (1) the threshold at which agents decide to communicate new cost maps and (2) the incremental rate of change in engagement cost. We examine how long it takes agents to desynchronize once an attack starts and how long it takes...
agents to resynchronize once an attack ends. Additionally, we consider the agent-threat distance during desynchronization. Altogether, we seek to extract trends from this data that offer insight into communication requirements for mission success. For example, we expect to gain an understanding of how quickly agents desynchronize under attack and how much time they require to resynchronize for effective engagement. This may in turn drive communication requirements (e.g., ability to detect and recover from failures within a critical time window) and help to prioritize usage of bandwidth-constrained or unreliable communication channels. That is, communication among agents in close proximity to a time-critical engagement may have highest priority for communication within their segment of the network.

B. Tactical Decision-Making Support

Metrics to link information attacks and mission effects equip combat system designers with tools to address risks from information operations. Without specifically designing counters for every possible information attack (a Sisyphean task), metrics such as commonality give designers a way to clearly quantify a level of performance that the combat system must achieve. They let designers know to what extent their information must be assured in order to achieve mission objectives. For example, in the design phase of a tactical decision-making algorithm, designers can determine what level of degraded commonality the algorithm tolerates. Designers can then work to increase the robustness of the algorithm and come up with alternate algorithms when information quality degrades too much. In addition, combat system designs can dynamically react to measures such as commonality. Reactions include detecting degraded information quality and switching strategies as well as taking steps to counteract the particular type of degradation currently being observed.

In order for combat systems to use metrics such as commonality, they must be able to measure the metric as operations unfold. Possible ways to collect these metrics include exchanging heartbeat messages to update the rest of the force on unit status. Parity-checking information can also be added to decision messages so that recipients can verify commonality of the information on which the decision is based. Units can also maintain a model of expected information quality given current operations. When expectations are not met, the combat system can then begin to suspect information operations.

Additionally, a combat system may be equipped to detect information degradation and switch engagement strategies accordingly. For example, a tactical-decision making system can switch to a decision scheme that is less reliant on information exchange. The secondary decision scheme may not be as optimal as the primary, but it should certainly be better than using the primary decision scheme under a level of information attack for which it was not designed. Combat systems can also use the detected level of information attack to calibrate information assurance strategies. For example, degraded information commonality could prescribe increased heartbeat messages or increased parity checking.

V. CONCLUSIONS AND FUTURE WORK

As the defense community increases reliance on net-centric operations, it becomes increasingly important to understand relationships between actions in the information space and their mission-level effect. We have presented initial progress toward a framework that links information operations and force-level results. We have quantitatively examined correlation among mission metrics and a variety of information metrics. We are in the initial stages of applying these insights to develop system-level IA requirements and tactical support strategies to decrease the impact of information attacks.

Our progress to date suggests several areas for future work. With respect to our current analysis, we will continue to refine our information metrics and identify good predictors of mission-level effects. We also seek to further validate our findings by performing higher fidelity simulations in environments such as ACES that consider force-level context for decision-making. We seek to expand our analysis to encompass additional attack conditions and scenarios that may provide insight into novel information metrics. Continued examination will also yield additional insight into requirements derivation and online tactical support.

REFERENCES