2014

Improving C2 Effectiveness Based on Robust Connectivity

S. Deller

A. Tolk
Old Dominion University, atolk@odu.edu

G. Rabadi
Old Dominion University, grabadi@odu.edu

S. Bowling

Original Publication Citation

Deller, S., Tolk, A., Rabadi, G., & Bowling, S. (2014). Improving C2 effectiveness based on robust connectivity. In T. J. Grant, R. H. P. Janssen, & H. Monsuur (Eds.), *Network Topology in Command and Control: Organization, Operation, and Evolution* (pp. 176-190). Hershey, PA, USA: IGI Global.

Chapter 8
Improving C2 Effectiveness Based on Robust Connectivity

S. Deller
Textron Defense Systems, USA

A. Tolk
SimIS Incorporated, USA & Old Dominion University, USA

G. Rabadi
Old Dominion University, USA

S. Bowling
Bluefield State College, USA

ABSTRACT

This chapter describes an approach to develop an improved metric for network effectiveness through the use of Cares' (2005) Information Age Combat Model (IACM) as a context for combat (or competition) between networked forces. The IACM highlights the inadequacy of commonly used quantifiable metrics with regards to comparing networks that differ only by the placement of a few links. An agent-based simulation is used to investigate the potential value of the Perron-Frobenius Eigenvalue (λ_{PFE}) as an indicator of network effectiveness. The results validate this assumption. Another measurement is proven to be equally important, namely the robustness of a configuration. Potential applications from the domain of ballistic missile defense are included to show operational relevance.

INTRODUCTION

The application of network theory enables us to investigate alternatives to the traditional hierarchical organizations of Command and Control (C2) processes and systems. Traditional hierarchical organizations were the result of centralized command and control cultures and the significant costs, both in time and money, of distributing the necessary information to enable sound decision-making. The increased desire for peer-to-peer negotiation and self-synchronization and the incredible reduction in these costs during the past decade has made non-hierarchical organizations viable alternatives. It also introduced a significant

DOI: 10.4018/978-1-4666-6058-8.ch008

challenge: what should we measure to determine which organization can be more effective?

The effectiveness of a C2 network is more than just the sum of its nodes and arcs, which can be measured by the *link-to-node ratio* (*l*/N). A maximally-connected network, where every node is connected to every other node (i.e., l = (N-1)!), not only remains prohibitive in monetary cost; it is undesirable due to the inability of a node to manage or process the overwhelming information flow represented by the arcs. However, a minimally-connected network may not be desirable due to either insufficient capability or capacity or an increased vulnerability of the network. Additionally, the *link-to-node ratio* metric cannot discriminate between alternative network organizations that have the same numbers of nodes and links, but differ solely in their arrangement. The mere counting of a link does not account for its significance, or lack thereof.

The *degree distribution* metric is a measurement of whether the number of links connected to each node is uniformly distributed throughout a network. Adaptive, complex networks have a small number of highly connected nodes (i.e., a skewed degree distribution). Such highly connected nodes can be clustered together or can be distanced from each other, and is expressed as a *clustering coefficient* calculated from the proportion of a node's direct neighbors that are also direct neighbors of each other. This represents a measurement of a network's cohesion and self-synchronization. The *characteristic path length* is a related metric, and is measured as the median of the mean of the lengths of all the shortest paths in the network. While these metrics begin to account for link significance, they are insufficient in discriminating between network configurations that vary in the placement of just a single link.

Jain and Krishna (2002) introduced the relationship between the Perron-Frobenius Eigenvalue (λ_{PFE}) of a graph and its autocatalytic sets, and used graph topology to study various network dynamics. Cares (2005) employed a similar approach to describe combat (or competition) between distributed, networked forces or organizations. His Information Age Combat Model (IACM) focused on the λ_{PFE} as a measure of the ability of a network to produce combat power. Cares proposed that the greater the value of the λ_{PFE}, the greater the effectiveness of the organization of that networked force.

Deller, et al (2009, 2012) confirmed this proposal by constructing an agent-based simulation that enabled networked organizations to compete against each other in the context of Cares' IACM. The results of the agent-based simulation indicated that the value of the λ_{PFE} was a significant measurement of the performance of a networked force. However, the effectiveness of the λ_{PFE} measurement was dependent on the existence of unique λ_{PFE} values for the configurations under consideration. When alternative organizations had a shared λ_{PFE} value, additional measurements were required to enable discrimination. Of the additional metrics considered, *robustness* proved the most effective in improving the value of the λ_{PFE} as a quantifiable metric of network performance. Ultimately, the best indicator of network effectiveness was a metric that combined both the λ_{PFE} and robustness values.

THE INFORMATION AGE COMBAT MODEL

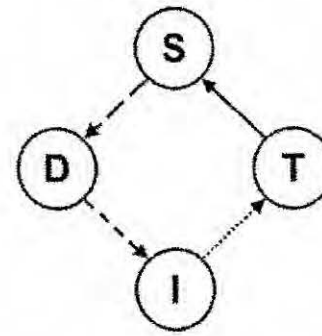
Cares designed the IACM to facilitate his investigation into how a networked force organizes. It is not intended to be a combat simulation or a tool to test weapon platforms. Instead, the basic objects of the IACM are generic nodes defined by the simple functions they perform, not by any performance specifications they were built or designed to. For example, Sensor nodes receive signals about observable phenomena of other nodes in the model. The types of signals received are not relevant; just that the Sensor "sensed" something about that node and passed that information on to a Decider node.

Decider nodes direct the actions of other nodes in the model. Likewise, the types of actions are not relevant; just that those other nodes take direction from that particular Decider (i.e., fall within that Decider's "command and control"). Nodes that interact with other nodes to affect the state of those nodes are called Influencers. Again, the types of interactions are not relevant, just that they may occur. Finally, those nodes that can be acted upon, but perform no sensing, deciding, or influencing functions are included as Target nodes. For the purpose of this discussion, all nodes belong to one of two opposing sides, conventionally termed BLUE and RED.

The links that connect these nodes represent the various physical and communicative interactions between them. Since these nodes perform a single function (e.g., "sense, "direct," etc.), information flow between the nodes is necessary for activity to occur, and generally takes the form of a combat cycle (see FigureFigure 1). In its simplest form, this cycle consists of a Sensor detecting an opposing node and passing that information to the Sensor's controlling Decider. The Decider may then direct one of its assigned Influencers to initiate action on the opposing node, such as exerting physical force, psychological or social influence, or some other form of influence. The effect of this action is subsequently detected by the Sensor and the cycle may be repeated until the desired outcome has been achieved. While the four links forming this cycle are just a small subset of the all the possible node-to-node permutations, they collectively represent the most important activity in the model and are the focus of this study.

All links in the model are directional, and have different meanings depending on which nodes they go "from" and "to". For example, a link from a Decider to any friendly node (whether it be a Sensor, Influencer, Target or other Decider) represents the conveyance of the Decider's direction (such as engagement or repositioning), but the links from an opposing Sensor and Influencer represent the Decider being detected and acted upon. Some links have two meanings, such as those from an Influencer to an opposing Sensor. These links represent two different interactions: detection and engagement. Both interpretations are valid and the context of the model will make clear which is intended.

Figure 1. Basic combat cycle



Other links have ambiguous meanings, such as those connecting Sensors of the same side. These can be defined as either the Sensors detecting each other or coordinating with each other. Links from a Sensor to other Sensors, Influencers, or Targets of the same side can be defined direct coordination but are not included in this discussion as it is assumed that the information detected must be routed through a friendly Decider. Additionally, links from an Influencer to other nodes of the same side represent fratricide and are not included either.

A collection of nodes and links can be described though the application of graph theory (Chartrand, 1984). A concise description of any graph is provided by the adjacency matrix A, in which the row and column indices represent the nodes, and the matrix elements are either one or zero according to the rule: $A_{ij} = 1$, if there exists a link from node i to node j and $A_{ij} = 0$, otherwise. Consequently, each unique network configuration of nodes and links has a unique mathematically-equivalent matrix portrayal. This enables the application of mathematical tools to analyze these networks, such as the Perron-Frobenius theorem. This theorem guarantees the existence of a real,

positive principal (maximum) eigenvalue of A_{ij} if A_{ij} is an irreducible nonnegative matrix. Since all the nodes on each side are connected to all the opposing Sensor and Influencer nodes, the matrix is strongly connected and, therefore, irreducible. This eigenvalue, λ_{PFE}, is a measure of the selective connectivity within the network (i.e., networks with the same number of links may have different λ_{PFE} values depending on the placement of the links). The full range of mathematical values for a λ_{PFE} of any adjacency matrix goes from 0 (for a network with no links at all) to n, where n = the total number of nodes (for a maximally connected network). Clearly, the λ_{PFE} is a quantifiable metric with which to measure the different ways to organize a networked force.

The λ_{PFE} is also an indicator of the effectiveness of that network's organization. This was determined through the construction of an agent-based simulation representing the IACM and the conduct of a series of force-on-force engagements to investigate the correlation of each opposing network's λ_{PFE} value with its corresponding probability of winning the engagement (Deller, et al, 2012). The opposing forces had equal assets and capabilities, but differed in their connectivity arrangements (i.e., where the links existed). These differences in connectivity often, but not necessarily, lead to unequal λ_{PFE} values.

The consideration of different λ_{PFE} values for the opposing forces reflects the first challenge in modeling the IACM. The IACM as originally described by Cares (2005) uses a single adjacency matrix to reflect the collective nodes and links of both BLUE and RED forces. This is sufficient when focusing on one side's organizational effectiveness while holding the other side constant. But BLUE and RED are each seeking separately to maximize their own organizational effectiveness, while at the same time minimizing the organizational effectiveness of the opposing force. This dynamic interaction cannot be accounted for with a single λ_{PFE} value, so we calculate separate values (λ_{BLUE} and λ_{RED}) to measure the potential effectiveness of each opposing configuration independent of the asset arrangement of the opposing force. Note, however, that these calculations required the adjacency matrices include a Target node to enable the complete depiction of any combat cycles the network configurations may contain. Any Target nodes included will be linked to all opposing Sensors (to enable potential detection) and Influencers (to enable potential action). While the number of Target nodes included affects the λ_{PFE} value, it does so because of the additional volume of nodes and links, not because of a difference in their configuration. Consequently, the use of a single Target node representative of all the enemy forces capable of being targeted can be assumed in order to focus on the aspect of the network that determines the λ_{PFE} value ordering.

The agent-based paradigm was utilized for this purpose because the resulting models provide both the ability to account for small unit organization and the autonomy of action that was necessary for our investigation. An additional advantage of utilizing an agent-based simulation was the ability to work around the ambiguities of link interpretation in the IACM described earlier. For details on the construct of the agent-based simulation see Deller, et al (2012).

The design of this experiment was intended to isolate the effect of the λ_{PFE} value by keeping as many variables between the forces as equal or constant as possible. The opposing forces consisted of the same number of Sensors, Deciders, and Influencers, differing only in how they were arranged (i.e., linked). Within each force, the numbers of Sensors and Influencers were equal to preclude any bias towards configurations that have more of one or the other, because the potential value of a Sensor may not truly equal the potential value of an Influencer. Consequently, the composition of each force followed an X-Y-X-1 (Sensor-Decider-Influencer-Target) template, with the sole target being representative of all the opposing nodes. Additionally, the performance capabilities of all Sensor and Influencer nodes within the agent-based simulation were identical (i.e., the sensing range equaled the influencing

range, and the speeds of movement for both types of nodes were the same).

The goal of this experiment was to gain a "first order" understanding of the IACM, therefore two key scoping decisions were made. First, each Sensor and Influencer would only be connected to one Decider (but any given Decider could be connected to multiple Sensors and Influencers). Second, the connectivity within any X-Y-X-1 force was limited to only those links necessary to create combat cycles (i.e., Target to Sensor, Sensor to Decider, Decider to Influencer, and Influencer to Target). These are the essence of the λ_{PFE}. Whereas the other link types can significantly enhance both the λ_{PFE} value and the performance of any given network configuration, the present model provides a baseline for assessing what the potential effects of that inclusion may be.

There are many ways in which nodes can be connected for specific values of X and Y. The number of possible configurations grows rapidly even for small values. Consider a tiny network consisting of three Sensors and three Influencers distributed between two Deciders. There are only four different permutations of the allocation of these Sensors and Influencers between these Deciders. However, because the nodes of the IACM are generic two of these four permutations are, in effect, isomorphic and therefore can be excluded (i.e., the only meaningful difference between these two possible configurations is whether the Decider that is linked to two Sensors is the same Decider that is linked to two Influencers. While this 50% reduction in combinations to be considered is trivial for this tiny network, it quickly becomes a crucial step in reducing the search space of the problem. Considering a slightly larger force of just five Sensors and five Influencers allocated across three Deciders yields 36 different permutations which, fortunately, can be reduced to eight meaningfully different configurations by applying the same logic.

As the size of the force is increased it is obvious that the contrast between the number of possible configurations and the number of meaningfully different configurations becomes extremely large very quickly. This disparity is further compounded by the comprehensive design of the experiment, where each configuration was tested against every possible configuration. Since a 7-3-7-1 network has 42 meaningfully different configurations this required 1,764 (i.e., 42^2) unique engagements. Had we not reduced the search space, we this would have required 50,625 (i.e., 225^2) unique engagements. The numbers of meaningfully different configurations for all X-Y-X-1 forces where X <

Table 1. The numbers of meaningfully different configurations of all X-Y-X-1 networked forces where X < 11 and Y < 8

		Number of Deciders (Y)				
		3	4	5	6	7
Numbers of Sensors (X) and Influencers (X)	3	1				
	4	2	1			
	5	8	2	1		
	6	19	9	2	1	
	7	42	27	9	2	1
	8	78	74	30	9	2
	9	139	168	95	31	9
	10	224	363	248	105	31

11 and Y < 8 based on the unique values for the distributions of Sensors and Influencers across the Deciders are summarized in Table 1.

As previously mentioned, each of these configurations has a unique adjacency matrix that represents the connectivity, or lack thereof, between each of the nodes. If we segment the adjacency matrix into parts by grouping the types of nodes together (as depicted in FigureFigure 2), we see that 14 of the 16 sections (the shaded areas in the figure) are homogenous, i.e. either all "1" or "0," due to the absolute absence or existence of any links between those types of nodes. The two unshaded sections reflect the connectivity of each Sensor and Influencer to and from a particular Decider, and vary by configuration based on the allocation of Sensors and Influencers across the Deciders. The effect of this near uniformity is to constrain the variance between the λ_{PFE} values to just a narrow portion of the full range of possible λ_{PFE} values. In the example case of a 7-3-7-1 network the full range of possible λ_{PFE} values varies between 0 (no connections) and 18 (maximally connected), but the actual range of λ_{PFE} values for the 42 meaningfully different configurations varies from 1.821 to 2.280.

Although the variation between the λ_{PFE} values is small, it is of significant utility because the values of other common statistical measures as defined by Cares (2005) remain constant between these configurations. The 42 meaningfully different configurations of a 7-3-7-1 network all have a link-to-node ratio of 1.556, regardless of where the links are placed. The characteristic path length and clustering coefficients are also constant across every configuration. These metrics can provide valuable insight regarding large, complex networks, but cannot discriminate between near-identical configurations of a smaller network, even

Figure 2. An adjacency matrix for one of the 42 meaningfully different configurations of a 7-3-7-1 network

To

From	S	S	S	S	S	S	S	D	D	D	I	I	I	I	I	I	I	T
S	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
T	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

if the only link changed has a significant impact on the effectiveness of that network.

Identical configurations of the same network always have the same λ_{PFE} value, but it is also possible for meaningfully different configurations to share the same λ_{PFE} value. In our example, the 42 meaningfully different configurations of a 7-3-7-1 networked force had only 13 unique λ_{PFE} values. When this occurs, the λ_{PFE} loses its utility as an indicator of potential performance between these configurations. Note that the numbers of unique λ_{PFE} values (shown in Table 2 for all X-Y-X-1 forces where $X < 11$ and $Y < 8$) increase at a significantly smaller rate than the numbers of meaningfully different combinations (shown in Table 1). This disparity has a significant impact on the analysis approach and results.

The initial experiment consisted of all possible force-on-force engagements of the 42 meaningfully different configurations of two 7-3-7-1 networked forces (BLUE and RED). These configurations had the same numbers of assets but differed only in the way nodes were connected, which will enable us to study the impact of connectivity on the network performance. To test the performance of each of these 42 configurations against each other required 1,764 different engagements were required with 30 replications of the agent-based simulation, each with a random distribution of the BLUE and RED nodes across the battlespace. The possible outcomes of each replication was a BLUE win, a RED win, or an undecided result.

The results showed that the greater the λ_{PFE} value for either BLUE or RED, the more likely that force would win the engagement. This trend is clear in FigureFigure 3, where the probability of a BLUE win for any particular configuration is averaged over all RED configurations. Note that the vertical groupings reflect those BLUE configurations that shared each of the 13 unique λ_{PFE} values. A linear regression model confirms the visual evidence with a coefficient of determination (R^2) of 0.896 for the following equation: $y = 1.0162(x) - 1.5780$, where y = the average probability of a BLUE win for that configuration and x = the λ_{PFE} value of a configuration.

The correlation between p(Win) and the λ_{PFE} value remains true for the 8-3-8-1 force as well. Adding just the one Sensor and Influencer increased the number of meaningful combinations to 78, with 24 unique λ_{PFE} values, with 6,084 different engagements to be tested (see FigureFigure 4). This linear regression resulted in a coefficient

Table 2. The numbers of unique λ_{PFE} values for the meaningful configurations for all X-Y-X-1 forces where $X < 11$ and $Y < 8$

		Number of Deciders (Y)				
		3	4	5	6	7
Numbers of Sensors (X) and Influencers (X)	3	1				
	4	2	1			
	5	4	2	1		
	6	8	4	2	1	
	7	13	8	4	2	1
	8	20	13	8	4	2
	9	27	20	13	8	4
	10	38	27	20	13	8

of determination (R^2) equal to 0.876 for the following equation: $Y = 0.9484(x) - 1.5633$, where y = the average probability of a BLUE win for that configuration and x = the λ_{PFE} value of a configuration.

The correlation between p(Win) and the λ_{PFE} value decreased significantly for a 9-5-9-1 force, however. The additional Sensor, Influencer, and Decider nodes increased the number of meaningfully different configurations to 95, and resulted in 9,025 different engagements to be tested. Surprisingly, the additional assets reduced the number of unique λ_{PFE} values to 13 (13.68%). This is a dramatic reduction from 30.77% (24 of 78) for the 8-3-8-1 force, and 30.95% (13 of 42) for the 7-3-7-1 force. The impact of this reduction in unique λ_{PFE} values is a greater variety of p(Win) across for each λ_{PFE} value (see FigureFigure 5); hence the reduction in R2 to a value of 0.519 for the resulting equation: $Y = 0.5861(x) - 0.7736$, where y = the average probability of a BLUE win for that configuration and x = the λ_{PFE} value of a configuration. Note that the highest p(Win) value does not belong to the configuration with the highest λ_{PFE} value, indicating that there is some other correlating factor in effect.

The most significant difference between the configurations sharing a common λ_{PFE} value concerns the balance of Sensors and Influencers for each Decider within that configuration. This balance defines the "robustness" of the configuration, which was a term used by Barabasi (2002) to describe a network's resilience to failure due to the loss of some of its nodes. Robustness can be defined here as the minimum number of nodes lost that would make the configuration ineffective (i.e., unable to destroy any more enemy nodes). Mathematically this can be expressed as: Robustness = $[\min(S_1, I_1)] + [\min(S_2, I_2)] + \ldots + [\min(S_n, I_n)]$, where S_n = the number of Sensors assigned to Decider *n* and I_n = the number of Influencers assigned to Decider *n*.

Figure 3. The average probability of a BLUE win by λ_{PFE} for 42 configurations of a 7-3-7-1 BLUE network

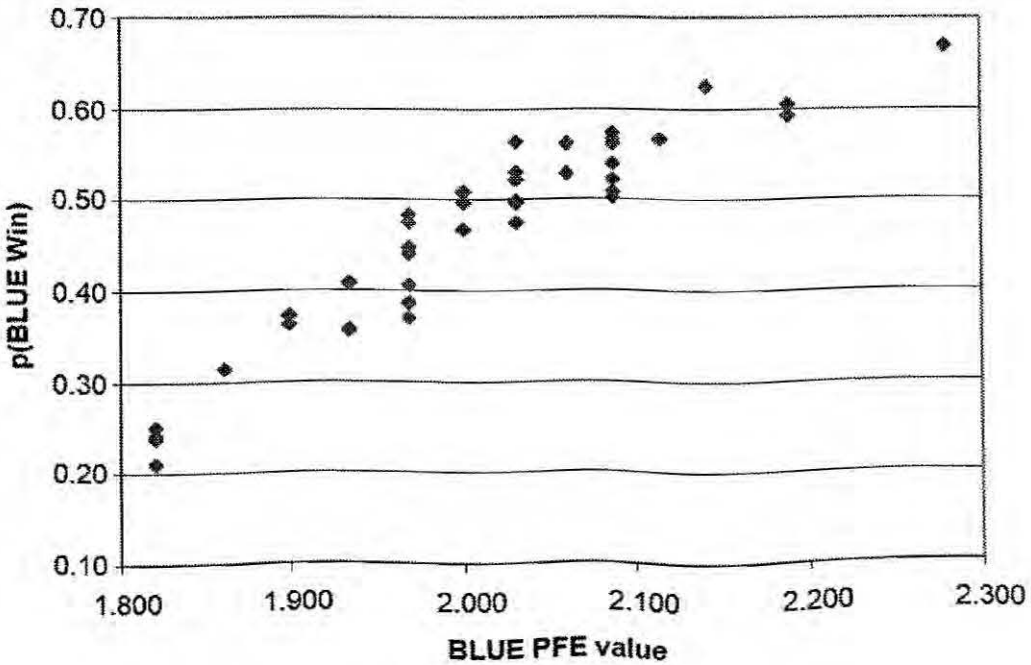
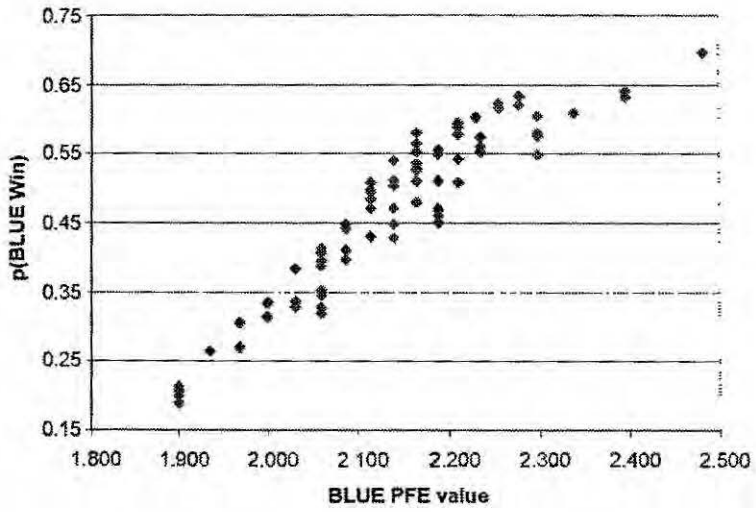


Figure 4. The average probability of a BLUE win by λ_{PFE} for 78 configurations of an 8-3-8-1 BLUE network



For example, a Decider has three Sensors but only one Influencer. This imbalance reduces the minimum number of nodes that can be lost before a portion of the force is rendered combat ineffective (i.e., unable to contribute due to the lack of combat cycles). If the sole Influencer is lost, then all three Sensors are combat ineffective as the information collected by the Sensors cannot be acted on. Essentially, the robustness value reflects the rate of the reduction of the λ_{PFE} value over time. The quicker a force can be rendered completely ineffective, the lower the robustness value. Configurations that were more robust generally had a greater probability of winning, while less robust configurations generally had a lower probability of winning (see FigureFigure 6).

Since the robustness value varied between configurations sharing the same λ_{PFE} value it be-

Figure 5. The average probability of a BLUE win by λ_{PFE} for 95 configurations of a 9-5-9-1 BLUE network

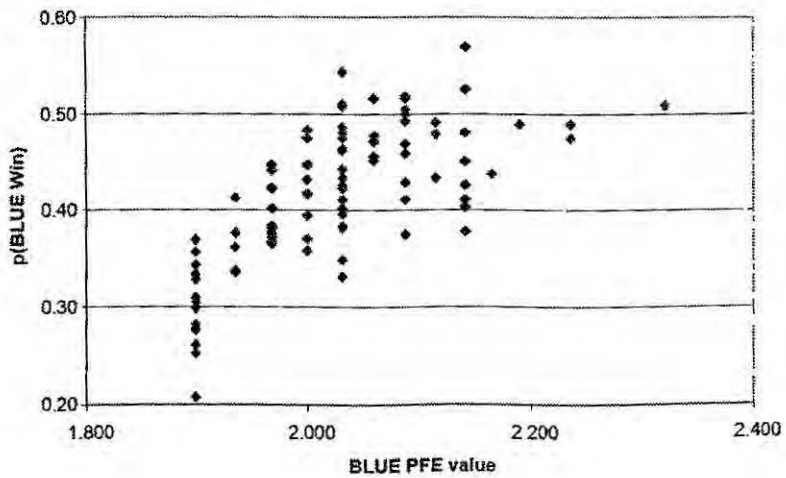
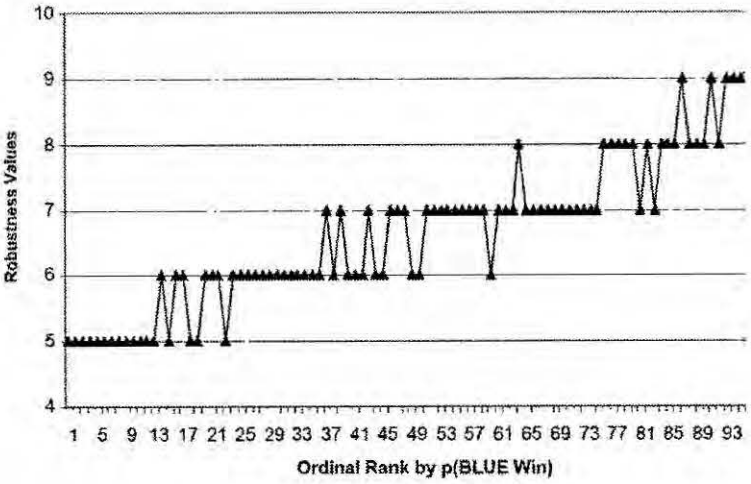


Figure 6. The robustness values of the 95 configurations of a 9-5-9-1 BLUE network



came a useful discriminator. For example, 20 of the 95 configurations of a 9-5-9-1 network share a λ_{PFE} value of 2.031, but their robustness values varied between 6 and 9. Of these 20, only one configuration had a robustness value of 9, and it was the one that scored the highest p(Win) value, 0.5425, which was significantly higher than the other 19 configurations. While there was a strong correlation between robustness and p(Win), it was not absolute: 3 of the configurations outperformed others that had a robustness value one greater. A regression analysis of both the λ_{PFE} value and the robustness value yields a significant increase in the coefficient of determination (R^2) from a value of 0.621 to 0.805 and provides the following equation: $y = [(-0.0307)(x_1) + 0.0615(x_2)] + 0.0678$, where y = the average probability of a BLUE win for that configuration, x_1 = the λ_{PFE} value of a configuration, and x_2 = the robustness value of a configuration.

APPLICATION FOR PRACTITIONERS

Due to the high costs and high risk of real system tests, the use of modeling and simulation instead of live tests and exercises has been recommended by Ender et al. (2010) and Garrett et al. (2011). Although the authors are not aware of any study on the efficiency of the ballistic missile defense system based on the principles of IACM, several studies have been provided that evaluate so called 'kill chains' or 'kill cycles' that have to be established in order to have efficient solutions (Holland and Wallace 2011). This study establishes a good use case for the approaches discussed in this chapter.

The challenges to design a reliable and secure defense system against ballistic missile attacks have been recognized and evaluated nationally (Fogleman 1995, Gompert and Isaacson 1999) as well as internationally (Yost 1982) for more than a decade. Recent political changes introduced additional constraints that require a high degree of interoperability between the systems and the detailed integration of command and control processes (Frühling and Sinjen 2010).

The general technical challenge remained the same since described in detail by Weiner (1984). The overall task is to destroy a hostile ballistic missile before it hits the target to be protected. To be able to do this, radars and other sensor means have to search for threats and detect them. Once a hostile missile is detected, it needs to be tracked

and a decision has to be made whether to target it or not. If the decision is positive, an interceptor has to be launched and guided into the target, followed an assessment if the engagement was successful or not.

Radar systems are space based, air based, and land based, with famous land based radar systems constructed close to the periphery of the alliance. The Cobra Dane Radar in Alaska, the Thule Radar in Greenland, and the Fylingdales Radar in the United Kingdom being examples. The US command centers Strategic Command (STRATCOM) and Northern Command (NORTHCOM) provide the Command, Control, Battle Management, and Communications (C2BMC) for the control. The interceptors are land-based Terminal High Altitude Area Defense (THAAD) Fire Units, sea-based Aegis Cruisers and Destroyers, and the land-based Patriot systems. Europe, Israel, and Japan are contributing their own components to support local concepts. The Missile Defense Agency, Army, Air Force, and Navy share responsibilities for operation, management, maintenance, and ongoing developments.

Holland and Wallace (2011) define a kill chain as a series combining all six main tasks to be conducted by the radar system, the control system, and the missile system. The proposed chain is displayed in Figure 7.

As identified by Garrett et al. (2011), the ballistic missile defense system is actually a system of systems in which the various components themselves are systems with established governance rules and that support the common objective of missile defense, but that are operationally independent. Overall, they fulfill the distinguishing characteristics compiled by Tolk, Adams, and Keating (2011):

- Operational independence of the systems,
- Managerial independence of the systems,
- Geographic distribution,
- Emergent behavior,
- Evolutionary development.

To establish a kill chain, components providing radar functionality to search and detect, control functionality to track, target, and assess, and missile functionality to engage are required to be interconnected via interoperable interfaces. Holland and Wallace (2011) identify scenario graphs to address what they refer to as integration readiness level: are the various components able to connect with each other in order to establish a kill chain, and are there redundancies to increase the stability of the ballistic missile defense operation. They use corresponding adjacency matrixes to identify which radar system connects with which control systems and which missile system.

This motivates, however, to map the ballistic missile defense components to the IACM components, eventually adding some extensions as discussed before: The hostile ballistic missile is the target T, the sensor provides the radar functionalities S, the decision nodes model the control functionalities, and the engaging interceptor missile system represents the influencer. The IACM interpretation of the kill chain is shown in the following figure.

This interpretation allows to apply the IACM insights described before to evaluate effectiveness and efficiency of the ballistic missile defense system. If each likely attack must be met by at

Figure 7. Kill Chain for the Ballistic Missile Defense System

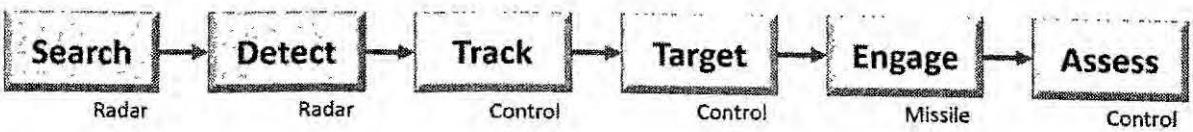
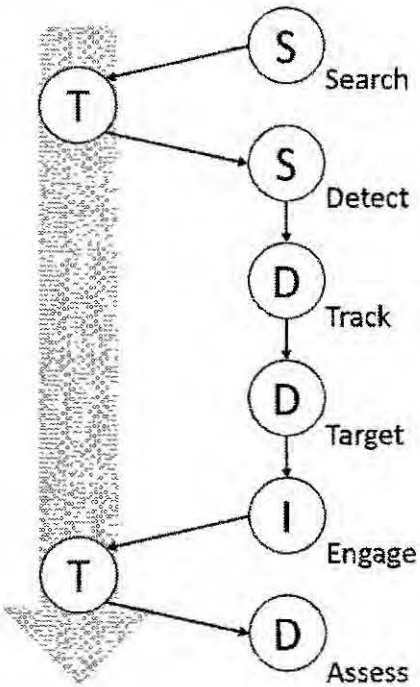


Figure 8. IACM Interpretation of the kill chain



least one kill chain. However, each additional kill chain increases the likelihood of a defense success, and the more kill chains can cover a target, the higher the defense success gets. The number of possible kill chains, however, can be captured by computing the eigenvalue λ_{PFE} of the resulting adjacency matrix resulting from the interpretation of interoperable components within the IACM.

The engagement step itself must also be interpreted as a kill cycle within the IACM. An interceptor fire unit comprises its own command and control center (D), a fire control radar (S), and the interceptor missile (I) to engage a hostile ballistic missile (T). In particular in combined operations in which several nations are fighting within a coalition, mutual support – like easily possible between two Aegis cruisers or two Patriot systems – is not the rule. The Israeli Arrow Weapon System, e.g., can be integrated into the kill chain using the C2BMC, but in the engagement cycle itself the fire unit components are not interchangeable, which is often a problem between services and sometimes even within the services as well. The kill cycle for the engagement step maps one-to-one to the basic combat cycle shown in FigureFigure 1 in the beginning of the chapter, although it should be pointed out that the tracking of the hostile ballistic missile by the fire control radar is a process, not an event. For high-level analysis as targeted within most contributions to this book, this level of detail is often negligible and it can be assumed that each fire unit can and will operate independently. Cross fire unit support can only increase the overall efficiency and has no negative effects on the overall performance of ballistic missile defense.

CONCLUSION

As recommended in the NATO Code of Best Practice for C2 Assessment (2002), the use of an orchestrated set of tools and methods is best practice when addressing complex questions like this one. The benefit of IACM based scenarios is that they allow us to analyze a broad volume of the solution space to identify a smaller fraction of particular interest. This smaller area can then be evaluated using detailed simulation systems, such as described by Lynch, Diallo, and Tolk (2013), which is based on the concepts theoretically introduced by Garrett et al. (2011).

The application of the IACM also shifts the focus of the assessment of a networked force from the capabilities of the nodes (generic in the IACM) to the capability of the network as a whole. The results of the agent-based simulation indicated that the value of the λ_{PFE} was a significant measurement of the performance of a networked force. We also learned that the λ_{PFE} value alone was insufficient indicator when the ratio of unique λ_{PFE} values for the configurations under consideration decreased. Other quantifiable network metrics, such as the link-to-node ratio, degree distribution, clustering coefficient, and characteristic path length, were unable to consistently discriminate between these configurations that differed by a single link, regardless of the significance of that link. The addition of a robustness factor was necessary to aid in predicting the network performance. By utilizing both the λ_{PFE} value and the robustness value, the coefficient of determination for the numerous configurations of three different networked forces showed a strong degree of correlation with the average probability of a Win.

We expect that these results will apply to even larger networks as well given that the only difference in the context of the IACM is a larger, possibly much larger, adjacency matrix. The mathematics of the application of graph theory remain the same. It is possible, however, that larger networks may have a smaller ratio of unique λ_{PFE} values. If so, the consideration of the robustness factor along with the λ_{PFE} value becomes even more necessary.

REFERENCES

Barabási, A. (2002). *Linked.* Perseus Publishing.

Cares, J. (2005). *Distributed Networked Operations.* New York: iUniverse.

Chartrand, G. (1984). *Introductory Graph Theory.* Dover Publications.

Deller, S. T., Bell, M. I., Bowling, S. R., Rabadi, G., & Tolk, A. (2009). Applying the Information Age Combat Model: Quantitative Analysis of Network Centric Operations. *The International Command and Control (C2). Journal, 3*(1), 1–25.

Deller, S. T., Rabadi, G., Tolk, A., & Bowling, S. R. (2012). Organizing for Improved Effectiveness in Networked Operations. *Military Operations Research Journal, 17*(1), 5–16. doi:10.5711/1082598317105

Ender, T., Leurck, R. F., Weaver, B., Miceli, P., Blair, W. D., West, P., & Mavris, D. (2010). System-of-Systems Analysis of Ballistic Missile Defense Architecture Effectiveness through Surrogate Modeling and Simulation. *IEEE Systems Journal, 4*(2), 156–166. doi:10.1109/JSYST.2010.2045541

Fogleman, R. R. (1995). Theater Ballistic Missile Defense. *Joint Force Quarterly, 9*, 75–79.

Frühling, S., & Sinjen, S. (2010). *Missile defense: challenges and opportunities for NATO.* NATO Defense College, Research Paper, 60: 1-5.

Garrett, R. K., Anderson, S., Baron, N. T., & Moreland, J. D. (2011). Managing the interstitials, a system of systems framework suited for the ballistic missile defense system. *Systems Engineering, 14*(1), 87–109. doi:10.1002/sys.20173

Gompert, D. C., & Isaacson, J. A. (1999). *Planning a ballistic missile defense system of systems.* RAND Report IP-181, 1-14.

Holland, O. T., & Wallace, S. E. (2011). Using Agents to Model the Kill Chain of the Ballistic Missile Defense System. *Naval Engineers Journal, 123*(3), 141–151. doi:10.1111/j.1559-3584.2011.00336.x

Jain, S., & Krishna, S. (2002). *Graph Theory and the Evolution of Autocatalytic Networks.* Retrieved from http://arXiv.org/abs/nlin.AO/0210070

Lynch, C. J., Diallo, S. Y., & Tolk, A. (2013). Representing the ballistic missile defense system using agent-based modeling. In *Proceedings of the Military Modeling & Simulation Symposium* (pp. 3-12). San Diego, CA: Society for Computer Simulation International.

NATO Code of Best Practice for C2 Assessment. (2002). Command and Control Research Program (CCRP) Press.

Tolk, A., Adams, K. M., & Keating, C. B. (2011). Towards Intelligence-based Systems Engineering and System of Systems Engineering. In *Intelligence-based Systems Engineering* (pp. 1–22). Springer. doi:10.1007/978-3-642-17931-0_1

Weiner, S. (1984). Systems and technology. In *Ballistic Missile Defense* (pp. 49–97). Brookings Inst Press.

Yost, D. S. (1982). Ballistic Missile Defense and the Atlantic Alliance. *International Security, 7*(2), 143–174. doi:10.2307/2538436

ADDITIONAL READING

Tolk, A. (2012). *Engineering Challenges for Combat Modeling and Distributed Simulation.* John Wiley and Sons. doi:10.1002/9781118180310

KEY TERMS AND DEFINITIONS

Ballistic Missile Defense System: A system of operationally independent systems that support the common objective of missile defense.

Command and Control (C2): The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Information Age Combat Model (IACM): A model, proposed by Cares (2005), of search, detection and attrition processes that is specifically designed to capture complex local behaviors, interdependencies and the skewed distribution of networked performance.

Kill Chain: A series of tasks that execute the following functions: search (sensor), detect (sensor), track (decision), target (decision), engage (influencer) and assess (decision).

APPENDIX

Questions

1. What other connectivity measures for matrices could be applied?
2. How will this observation change if connections are no longer sure (p=1.0) but only likely ($0 < p < 1$), e.g. when detection probabilities or communication probabilities are modeled in the IACM?
3. Can Kill Chains as described for the BDMS example be expressed in form of matrices?
4. Can we determine the value of a Sensor relative to an Influencer?
5. How many assets can organizational optimization offset (i.e. a smaller, more optimally organized force defeating a larger force)?

Managing Director: Lindsay Johnston
Production Editor: Jennifer Yoder
Development Editor: Austin DeMarco
Acquisitions Editor: Kayla Wolfe
Typesetter: James Knapp
Cover Design: Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Grant, T. J., 1947-
Network topology in command and control : organization, operation, and evolution / T.J. Grant, R.H.P. Janssen, and H. Monsuur.
pages cm
Includes bibliographical references and index.
Summary: "This book connects the fields of C2 and network science, featring timely research on topics pertaining to the C2 network evolution, security, and modeling"-- Provided by publisher.
ISBN 978-1-4666-6058-8 (hardcover) -- ISBN 978-1-4666-6059-5 (ebook) -- ISBN 978-1-4666-6061-8 (print & perpetual access) 1. Command and control systems. 2. Electric network topology. I. Title.
UB212.G73 2014
355.3'3041--dc23

2014007809

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.