中国电子学会电子系统工程分会
第十三届信息化理论学术研讨会论文集

信息化理论与综合信息系统

信息化理论学术研讨会论文集编委会 编

安徽大学出版社

中国电子学会电子系统工程分会
第十三届信息化理论学术研讨会论文集

信息化理论与综合信息系统

信息化理论学术研讨会论文集编委会 编

安徽大学出版社

图书在版编目(CIP)数据

信息化理论与综合信息系统:中国电子学会电子系统工程分会第十三届信息化理论学术研讨会论文集/信息化理论学术研讨会编委会编. ——合肥:安徽大学出版社,2006.10

ISBN 7-81110-219-6

Ⅰ.信… Ⅱ.信… Ⅲ.信息技术—学术会议—文集 Ⅳ.G202-53

中国版本图书馆 CIP 数据核字(2006)第 120764 号

出版发行	安徽大学出版社	**经　销**	新华书店
	(合肥市肥西路 3 号 邮编 230039)	**印　刷**	合肥寿春印刷有限公司
联系电话	编辑室 0551-5766417	**开　本**	850×1168　1/16
	发行部 0551-5107784	**印　张**	24
电子信箱	ahdxchps@mail.hf.ah.cn	**字　数**	550 千
责任编辑	李镜平　李　宗	**版　次**	2006 年 10 月第 1 版
封面设计	李　梅	**印　次**	2006 年 10 月第 1 次印刷
	ISBN 7-81110-219-6/T・99	**定　价**	80.00 元

前　言

我军信息化建设已进入了一个新的时期。以新时期军事战略方针为指导思想，着眼于提高我军的整体作战效能和信息化水平，坚持一体化的发展道路，适应高技术条件下作战的需要，尽快缩短与世界上发达国家之间的差距，立足于“打赢”，使之成为在未来信息作战中与强敌对抗的“杀手锏”，是我军信息化建设的发展方向，是适应新形势下我军信息化建设工作需要的要求。根据中国电子学会电子系统工程分会的工作安排，在全军信息化工作办公室和中国电子学会电子系统工程分会的指导下，信息化理论学组于2006年10月在安徽召开第十三届学术研讨会。研讨会以指挥自动化与信息安全为主题，探讨了指挥自动化系统综合集成建设的对策与建议、综合集成工程的理论与实践、综合集成的需求工程与数据工程、指挥自动化系统的作战体系结构、系统体系结构和技术体系结构、信息融合的理论、技术和应用、信息作战指挥自动化理论、信息作战指挥自动化系统建设的理论与实践、信息作战辅助决策系统的理论与方法、网络安全技术、网络基础设施与资源建设、网络仿真模拟训练系统体系结构理论方法和应用技术等方面的问题。

本届年会共收到论文153篇，经论文评审专家组审定，决定录用102篇，并汇集成册，由安徽大学出版社正式出版。论文集分为信息化理论、建设与C^3I体系结构、信息对抗与信息安全、军事信息系统设计理论与方法和信息化建设相关技术四大部分，每部分按内容分类编排，其先后顺序不反映任何优先级别。希望本论文集能对从事我军信息化工作的同志有所帮助。

本论文集编辑过程中，得到了电子系统工程分会、总参61研究所、国防科技大学、解放军理工大学、西安电子科技大学等单位的大力支持，尤其是本届年会承办单位电子工程学院的领导、科研部机关和网络工程系给予了热情指导和鼎力帮助。论文的评审、编辑和出版得到了电子工程学院学报编辑部的大力支持，他们为此做了大量的工作，付出了艰辛的劳动。在此一并表示感谢！由于时间仓促，对论文的少量修改未能与有关作者商酌，编辑过程中的错误在所难免，恳请论文作者和读者批评指正。

信息化理论学术研讨会论文集编委会

二〇〇六年十月于合肥

目　　次

信息化理论、建设与C³I体系结构

信息对抗与信息安全

军事信息系统设计理论与方法

信息化建设相关技术

C^4ISR 系统态势感知框架及评估指标研究

赵　策[1]　张金辉[2]　刘千里[3]　杨俊强[4]
(1. 解放军理工大学指挥自动化学院；2. 解放军总医院通信站；
3. 总参第六十一研究所通信研究中心；4. 西安通信学院)

摘　要　获取和维持精确的战场态势信息是 C^4ISR 系统的基本功能之一。在信息化作战条件下，依托战术互联网构建有效的指挥信息网络态势感知框架，不但可以充分利用战术互联网灵活、机动、高效的特点，还可以增强整个指控系统的态势感知能力。本文首先给出了态势感知框架的概念，并在分析了态势感知信息特点的基础上，结合传统评估方法定义了针对态势感知框架的几个新的评估指标并做出了定量的描述。同时还根据美军 C^4ISR 系统态势感知能力的研究、发展现状，针对美军 21 世纪部队旅及旅以下指挥系统(FBCB2)做了相应的介绍。

关键词　C^4ISR 系统，战术互联网，态势感知，系统框架，评估指标

信息化作战条件下，随着作战单元机动性的不断提高，指挥机关对战场态势感知信息的精确性和实时性提出了更高的要求。作为信息化战场中数字化部队机动作战的信息基础设施，战术互联网(Tactical Internet，TI)的主要功能之一就是提高己方战场中独立作战单元的态势感知(Situational Awareness，SA)能力。在战场环境下准确、及时地掌握敌我友军的位置，不但可以减少误伤事故，提高打击的精确度，还可以为计划制定和决策提供有益的信息。态势感知信息的传输，以及对友军所掌握态势信息的融合都要利用网络来完成，这就需要以战术互联网为基础构建能够提供有效、可靠的传输数据并能够适应 SA 信息传输特点的通信网络框架，这就是态势感知框架(SA Architecture)。

由于态势感知框架是在战术互联网的基础上搭建的，因此通信网效能评估的基本指标也适用于对态势感知框架的评估。然而，在利用传统的通信网评估指标对态势感知框架进行评估时，会遇到很多传统指标无法衡量的问题，特别是对态势感知信息的精确性和实时性的评估，传统的通信网评估指标就不能满足要求。因此，本文结合态势感知信息的特点提出了平均 SA 寿命和平均 SA 准确度两个指标，来解决态势感知信息实时性和精确性的评估问题。

1　态势感知信息与态势感知框架

1.1　态势感知信息及其特点

态势感知信息是战场中敌我友部队情况的综合，是基于层次和位置关系的最新战斗信息，主要包括：敌我友各军兵种部队的位置信息，战区内地图、地形和海拔数据等，同时还包括了布雷区、后勤物资仓库、核生化武器沾染区等基本战场态势数据。获取和维持比较精确的战场态势信息，不但可以为各类军事行动提供信息优势保障，同时还可以极大增强决策机关的指挥控制(Command and Control，C^2)能力。SA 信息同 C^2 信息一样通过战术级指挥信息网络进行分发和传输。

态势感知信息是对时间和传输距离高度敏感的信息，只有实时的战斗单元位置报告才能形成精确的战场态势图。因此，态势感知框架的设计应着重考虑网络的可靠性、有效性以及较高的态势图传输速率。态势感知框架的设计与其他信息系统的设计有很大的区别，最主要的是在态势感知框架结构中，各传感器或独立作战单元会以很高的频率发送探测到的敌我友战斗单元位置信息(简称位置信息)，因此，即使某条位置报告信息在网络传输过程中丢失，也会因为后续位置信息的更新而不会对整个战场态势图的精确性产生致命的影响。这意味着对于 SA 信息的传输可以考虑

以牺牲一定的可靠性来换取更高的传播速率。这样的方案与 C^2 信息的传输是有区别的,因为在通常情况下,C^2 信息由于包含十分机密、敏感的内容而不会频繁的重复发送,因此在传送 C^2 信息时,即使出现很少比特的丢失也会使整个传输过程失败。

结合态势感知信息的特点我们可以发现,通常情况下传统的网络性能指标只用于评估网络硬件设备以及各类网络协议的可靠性和有效性,而其不能很好的描述态势信息的精确性和有效性的根本原因在于:目标单元的移动性和网络传输的时延在很大程度上产生了目标单元位置信息的不准确性,而利用传统网络性能指标无法衡量这种不准确性。

1.2　态势感知信息及其特点

战术互联网作为信息化战场 C⁴ISR 系统基本的通信网络,为态势感知信息的传输和分发提供了基本的网络环境。为适应态势感知信息的传输和分发,在战术互联网基础上采用层次化的框架结构构建态势感知框架,如图 1 所示,基本态势感知框架图包含了两个级别的态势感知网络,其中骨干 SA 网为上层网络,本地 SA 网为下层网络,两层网络中间的融合服务器起到了数据融合以及网关的作用。美军在其 21 世纪部队旅及旅以下战术指挥系统 FBCB² (Force XXI Battle Command Brigade-under Brigade)中的战术互联网系统中也采用了类似的结构来支持其 C⁴ISR 系统态势感知信息的分发。

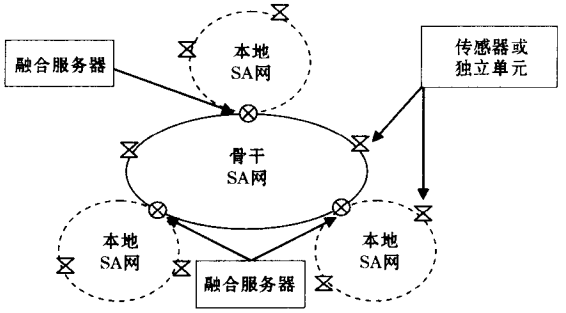

图 1　基本态势感知框架图

2　美军态势感知框架的典型应用

美国陆军的 21 世纪部队旅及旅以下作战指挥(FBCB²)系统是一个自动化、数字化的作战 C⁴ISR 系统网络,主要用途是为旅及旅以下部队直到单个战斗平台和单兵,提供运动中实时和近实时的 C^2 和 SA 信息;为指挥员、侦察分队和单兵提供精确的敌我位置显示;收发作战命令和后勤数据;进行目标识别等。在伊拉克战争中,FBCB² 首次投入实战,为作战部队提供了其他任何系统难以比拟的战场态势感知能力,对作战指挥起到了非常重要的作用。

在战场态势感知能力方面,FBCB² 可以看作是一套稳定的数字无线信息传输系统,其战场信息传输系统主要采用了两条视距通信系统——移动用户设备(Combat Net Radio/Wireless LAN, CNR),为作战车辆和指挥所配备的计算机系统提供数字化信息;战术互联网系统(SINCGARS/EPLRS),作为旅以下分队主要的战场态势感知和信息分发手段。FBCB² 系统的态势感知框架就是在上述两套通信系统平台上构建的,如图 2 所示。

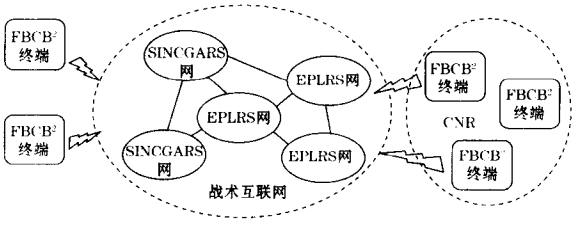

图 2　FBCB² 系统态势感知结构图

其态势感知软件能够显示战场上的单兵、武器平台、指挥所以及其他的投入战斗设施的地理位置信息;并允许陆军地面车辆、飞机和指挥中心近似实时地看到同一幅综合战场态势图;为适应网络中心战的概念,该系统也允许战场范围内横向和纵向的所有作战单元都能够实时或接近实时的共享全部的或根据任务需要定制的战场态势信息。同时,FBCB² 能够通过战术互联网根据战区内装备 FBCB² 终端的各单元输入的信息不断更新战场态势图。

3　态势感知能力评估指标

在战术互联网态势感知框架的评估中,建立一套合适的指标体系十分重要。美军旅及旅以下单位战术指挥系统 FBCB² 的数字化战场通信模型(DBCM)的建模与仿真小组已经开发出了适合

于态势感知框架的通信系统效能评估模型,并利用该系统对 FBCB² 的几种态势感知框架方案进行了评估。由于战术互联网态势感知框架不但具有一般战术通信网络的基本结构,同时又具有自身的特点,因此在选择评估方法和指标时不但应该使用传统的效能评估方法和指标,如端到端时延、吞吐量等指标;同时,也要针对传统的指标在评估战场态势图精确性上的不足,确定新的评估方法和指标。

3.1　平均 SA 寿命

SA 寿命(SA Age)的定义是指挥员主观认为某作战单元仍然在态势信息中汇报位置的持续时间,这个时间间隔以态势发送单元发送一个态势信息作为开始,以态势接收单元接收到一个新的态势信息作为结束。图 3 从时序角度对 SA 信息的寿命做出了直观描述。由于在整个仿真过程中,网络中产生的每组 SA 信息均具有其相应的 SA 寿命。因此,从记录和评估的角度出发,我们引入了平均 SA 寿命的概念。

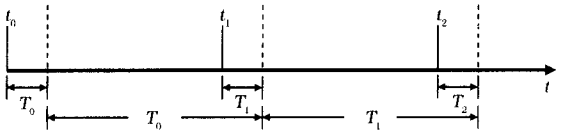

图 3　SA 寿命计算时序图

由图 3 可知:设 $t_0, t_1, t_2, \cdots, t_n$ 为某态势感知信息发送单元(简称发送单元)产生态势信息的时刻;$T_0, T_1, T_2, \cdots, T_n$ 为网络时延,即从态势信息产生到其被态势感知信息接收单元(简称接收单元)正确接收的时间间隔,网络时延主要由发送队列排队时延、发送时延和传播时延组成;T_0, $T_1, \cdots, T_n$ 为接收单元收到连续两个态势信息的时间间隔。则由定义可知时序图中描述的平均 SA 寿命的计算公式为:

$$AG' = \left(\frac{T'_0 + T_0}{2}\right) \cdot \left(\frac{T'_0}{T'_0 + T'_1}\right) + \left(\frac{T'_1 + T_1}{2}\right) \cdot \left(\frac{T'_1}{T'_0 + T'_1}\right) \tag{1}$$

式(1)给出了网络中两个态势感知单元产生、传输态势信息时 SA 寿命的计算方法。然而在实际的网络中,每个网络节点均可以看作是态势感知单元。假设网络中有 3 个感知单元 N_1、N_2、N_3,那么在整个网络中将产生和维持 6 个 SA 寿命值,分别是 N_1 与 N_2、N_3 之间产生的 2 个 SA 寿命值,以及依此类推 N_2、N_3 各自产生的 SA 寿命值。根据以上假设,若网络中有 n 个节点,则应有 $n(n-1)$ 个 SA 寿命值存在,同时可将式(1)推广为网络的平均 SA 寿命值:

$$AG_{avg} = \sum_{i=1}^{n} \left(\frac{T'_i + T_i}{2}\right) \cdot \frac{T'_i}{T'_n} \tag{2}$$

其中,$T'_n = \sum_{i=1}^{n} T'_i$,　$i = 1, 2, \cdots, n$。

在对战术互联网进行仿真的过程中,要对各节点的 SA 寿命值做持续的全过程的采集,在仿真结束后根据公式计算该网络对应的平均 SA 寿命值。

在定义和描述了战术互联网的平均 SA 寿命值后,可以扩展的给出网络的平均最长 SA 寿命值。这个值可以通过计算网络中所有节点各自的最长 SA 寿命,并取这些值的算数平均值得到。

3.2　平均 SA 准确度

SA 准确度(SA Accuracy)定义为某个探测目标在某一时刻的实际位置与接收单元接收到最新态势信息中报告的该单元位置的差值。根据定义可知 SA 准确度是以距离为单位的变量,可以通过计算态势感知单元的平均 SA 寿命与其移动速度 V(假设所有节点都以匀速运动)的乘积而得到,且准确度的值越小,则 SA 信息的精确性越高。如式(3)描述:

$$AC[\mathrm{m}] = \frac{AG[\mathrm{s}] \cdot V[\mathrm{km/h}] \cdot 1000[\mathrm{m}]}{3600[\mathrm{s}]} \tag{3}$$

3.3　态势信息交付率

态势信息交付率(Message Completion Rate, MCR)定义为网络能够成功完成态势信息的传输(或称为成功交付)的能力。MCR 是某接收单元实际接收到态势信息的数量与所有节点向网络提交的各类的态势信息的总数之比。若计算整个网络的 MCR 则需要使用所有接收单元接收到态势信息的数量,即:

$$MCR_n = \frac{n\text{个节点正确接收到的态势信息数}}{\text{感知单元向网络提交的所有态势信息数}} \tag{4}$$

4　引入评估指标的应用

在实际应用中,通常采用 SA 寿命和 SA 准确度两个指标来评估战术互联网态势感知框架的有效性。一个有效的态势感知框架必须具有能够

及时、有效地维持和更新战场动态单元态势信息的能力。随着时间的推移，已掌握的态势信息（特别是目标的位置信息）变得越来越不精确，即位置误差变大了。SA 寿命指标就给出了定量描述己方掌握的位置信息与实际目标位置之间误差的度量方法。

通常情况下，指挥机关更希望得到 SA 寿命值相对较短的 SA 信息。短寿命的 SA 信息意味着战场内各目标的位置信息更加精确，由这样的 SA 信息形成的战场态势图更能反映实时的战场态势。然而，仅依据 SA 寿命指标并不能全面反映战术互联网态势感知框架的有效性。例如一个目标单元的移动不是十分频繁，则该单元 SA 信息的寿命值相对就较长，但其精确性却依然很高的，这时需要引入 SA 准确度指标。SA 准确度指标是在考虑 SA 寿命指标的条件下，结合目标单元的移动速率而形成的以距离为单位的评估指标。指挥所的信息融合系统通过计算 SA 准确度来判断在接收到的某目标单元 SA 寿命值很大的情况下，是否会对整个战场态势图的精确性产生大的影响。

对于发送单元而言，保持较短 SA 寿命的方法可以是增加发送 SA 信息的数量和频率。然而这种方法也有局限性，在增加 SA 信息数量的同时也会占用更多的信道带宽，甚至会导致信道资源的枯竭。从这个意义上来说，提高 SA 信息的发送频率不但不能降低 SA 信息的寿命，反而会在有限的信道资源中产生更多的碰撞以及更长的发送队列排队时延。对于这个问题可分两种情况来处理：对于移动速度较慢的目标单元，可以降低 SA 信息的发送频率；对于移动速度较快的目标单元，可以适当的提高 SA 信息的发送频率。采用这种方法可以提高整个态势感知信息及战场态势图的精确性。通过引入 SA 准确度，监测人员可以发现哪个目标单元需要被赋予更高的 SA 信息发送速率；同样，可以更加有效的利用有限的战场通信资源，来达到提高整个战术互联网态势感知框架效能的目的。

然而，SA 寿命和 SA 准确度并不适用于对所有类型的 SA 信息进行评估，它们主要用于评估需要频繁更新的以及对移动性要求很高的 SA 数据。例如，我们在对某类态势感知框架进行评估时，SA 寿命和 SA 准确度主要用来分析和计算敌我双方战斗单元的位置数据而不是战区范围内的地形资料。

5　结束语

战场态势感知能力作为部队信息化作战能力的重要组成部分，已经成为夺取战场信息优势的重要保证。利用战术互联网构建的指挥信息网络态势感知框架可以充分利用战术互联网提供的无缝连接的能力，优化和提高整体参战部队的态势感知能力。本文提出的态势感知框架评估指标能够更加客观、全面的对 C⁴ISR 系统信息网络态势感知能力进行评估。下一步可以结合上述评估指标，对态势感知框架进行建模与仿真，在仿真环境下设计更加符合实战环境要求的态势感知框架，实现对网络硬件，软件和协议的最佳利用。

参 考 文 献

[1] 王海涛，等. 战术互联网的主要装备、关键技术和未来发展. 航空电子技术，2005(1).

[2] 王剑飞，等. 网络中心战中的美国海军 C⁴ISR 系统效能评估. 指挥控制与仿真，2005(5).

[3] 张自维. 等. 信息系统效能评估的一种方法. 工业控制计算机，2004(9).

[4] 方秀花，等. FBCB² 系统的作战应用及未来发展. 火力与指挥控制，2006(3).

[5] 陈绍顺，等. 战场态势的定量分析模型. 指挥控制与仿真，2004(6).

[6] Paul Sass. Communications networks for the Force XXI Digitized Battlefield. Mobile Networks and Applications，1999.

[7] Alex White. Modeling and Simulation of SA in FBCB2. MILCOM-IEEE，1998 年 10 月.

GIG 体系结构作用浅析

蒋园园　宋自林　苏云霞　马怡佳
（解放军理工大学指挥自动化学院）

摘　要　GIGv1.0 与 GIGv2.0 是 GIG 体系结构开发在不同阶段的产物，具有不同开发目的与作用。本文首先分析了 GIGv1.0 的体系结构集成可行性验证方面的作用，然后分析了 GIGv2.0 对于网络中心行动与作战的支持作用，并在其中对两者进行了适当的比较。

关键词　GIG，体系结构，体系结构集成，体系结构框架，网络中心信息域

0　概述

系统的体系结构是对该系统基本构造的概念化呈现，是用图、表和文字等方式对其组成部分，各组成之间的关系，系统与环境之间的关系，以及指导系统设计与演化的原理的表示。1996 年，为了改善美国联邦信息技术资源的选择与管理方式，美国国会与总统联合签署并颁布了克林格·科恩法案。在这项法案中指出，一个执行机构的信息技术体系结构是这个机构为了实现其战略目的与信息资源管理目标而发展或维护其现有信息技术，并且采购新的信息技术的一个集成框架。

GIG 体系结构的开发是美国国防部对克林格·科恩法案的一个响应。美国国防部于 2001 年和 2003 年相继推出了 GIGv1.0 与 GIGv2.0，它们在目标与用途上具有本质的区别。概括说来，GIGv1.0 立足于当前的联合作战环境，是一个范围虽小，但结构完整的集成体系结构。其目的是作为一个体系结构原型来验证使用 C⁴ISR 体系结构框架可以有效地将现有各异的体系结构集成为一个单一的体系结构。与 GIGv1.0 相比，GIGv2.0 立足于目标网络中心环境，是一个覆盖战略、战役、战术和合成作战的最终版体系结构。其目标是确定美国各司令部、各军种和国防部各厅局在网络中心信息环境遂行或支持作战与行动所需的 GIG 企业级能力。打个比方，如果说 GIGv1.0 是小规模的实验，那么 GIGv2.0 则是大规模的生产。

GIGv1.0 使用 C⁴ISR 体系结构框架 2.0 版本开发，GIGv2.0 则使用国防部体系结构框架 1.0 版本（DoDAFv1.0）。DoDAFv1.0 是对 C⁴ISR 体系结构框架 v2.0 的继承与发展。

1　GIGv1.0：体系结构集成的可行性验证

GIGv1.0 是开发企业体系结构的第一步，它的作用是为将现有的各种不同的体系结构集成为一个单一的，遵循框架的体系结构描述建立可行性。其体系结构集成具体表现在体系结构视图的集成与跨体系结构集成两个方面。

1.1　体系结构视图的集成

GIGv1.0 是一个综合了作战视图、系统视图和技术标准视图的单一的体系结构描述。GIGv1.0 根据 C⁴ISR 体系结构框架开发。根据这一框架，根据分析角度的不同，可以将对系统的分析分别组织成这三种相互关联的体系结构视图。其中作战视图描述的是完成或支援军事作战所需的任务和行动、作战要素和信息流；系统视图描述的是支持作战功能所需的系统及其连接；技术视图描述的是对于系统各部件或要素的排列、交互作用和相互依赖性的一组最基本的规则。

每一种视图都由一组特定的、相互关联的产品组成，分别形成一个完整的体系结构，而这三个体系结构视图之间则通过公共的参考点连接。比如，SV－5 将作战活动模型（OV－5）中的作战活动与 SV－4 中的系统功能相关联，从而联结了作战视图与系统视图。技术标准简档（TV－1）中的标准在特定的系统产品（如网络协议和系统数据交换）中都有列举，从而联结了系统视图与技术视图。

1.2 跨体系结构集成

关注不同的功能域、使命域或作战级别可以相应地建立具有不同规模与范围的体系结构,如精确打击、战场情报收集等功能域体系结构,指挥控制、后勤支援等使命域,还有战略、战役级、以及战术级体系结构等。这其中每一个都是包含作战视图、系统视图与技术视图的完整的体系结构。将这些体系结构集成为覆盖范围更大或跨越多个作战等级的体系结构就称为跨体系结构集成。

在 GIGv1.0 中最为典型跨体系结构集成是基于想定的作战视图体系结构。它将现有的联合作战体系结构、首席参谋助理体系结构和中央司令部网络运行体系结构集成为一个单一的、内容一致的作战视图体系结构,覆盖了联合作战活动中涉及到的不同功能与业务领域。其中以联合作战体系结构为核心。

联合作战体系结构表示的是应用于每一个联合作战人员(即各战斗司令部与联合特种部队)的一组关键的标准作战能力,以及联合军事行动的执行环境。它选择了 7 个具有代表性的联合使命域,如火力运用、指挥与控制、情报侦察与监视等,并将它们分别所代表的体系结构集成为一个单一的联合作战体系结构。首席参谋助理体系结构用于描述国防部首席参谋助理对于作战的支持,以及在这过程中所涉及到的,与之有关的信息交换。它选择了四个首席参谋助理来限定体系结构的范围。这四个首席参谋助理分别是负责人事与战备的国防部副部长,负责卫生事务的国防部长助理,负责审计的国防部副部长和负责采购、技术和后勤的国防部副部长。它们为作战行动提供其业务领域内的支持。网络运行体系结构关注的则是电信网络管理、信息分发管理与信息保障管理领域的事务。

这三个体系结构之间的关系可以简单的从以下的 GIGv1.0 高层作战概念图(图 1)来表示。

这张根据想定制定的高层作战概念图指出了所有参与或支持作战的节点,以及它们之间的关联。在图的左下角和右上角分别标出了所集成的体系结构。这些体系结构能够集成的关键在于它们都是在同一个框架结构内开发的,不但使用同样的产品进行描述,而且也统一了体系结构元素(如作战节点、作战活动、系统或物理节点、信息交换等)的定义,使得同一个体系结构元素能够在不同的体系结构或不同的视图中都能找到一致的对应。第二,开发了链接体系结构,用于识别跨功能边界的信息流,并支持互操作能力的评估。第三,通过想定事件,将各个体系结构所代表的领域联系起来,从而建立信息交换关系。GIGv1.0 为下一步目标体系结构的开发提供了一个样本,它保证了使用这样的方法开发能够得到一个集成的体系结构。此外,在 v1.0 的开发过程中,开发人员也总结了开发的经验与教训,保证了下一步开发工作的顺利展开。

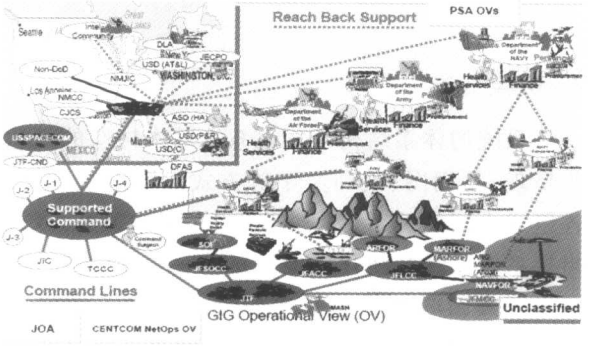

图 1 GIGv1.0 高层作战概念图

2 GIGv2.0:NCOW 的企业体系结构

GIG 是实施网络中心战(NCOW)的信息基础设施,对于 GIG 的体系结构来说,其最终目的是以网络中心战为出发点来描述 GIG 在一个网络中心环境中的企业需求,识别 NCOW 在战略、行动、战术与合成作战中的企业信息技术含义,并最终生成 NCOW 的体系结构模型。因此作为 GIG 体系结构最终版的 GIGv2.0 是 NCOW 的企业体系结构。

GIGv2.0 由五个 Block 体系结构组成,每一个 Block 都是一个具有特定范围和关注点的、与某一作战与决策层次相关的体系结构。下面将以 Block4 为例,说明 GIGv2.0 对于 NCOW 的支持。Block4 体系结构是关注的是在战术层执行 NCOW 对于 GIG 的企业需求,是一个由作战视图、系统视图与技术视图组成的完整的体系结构。

2.1 网络中心信息域

在图 2 中,全球信息栅格以遍布全球的网格表示;参与作战行动的人员、组织机构、平台或设

施等都以接入栅格中的节点表示,亦称之为作战节点;而节点之间的连线则表示它们之间的信息交换关系。

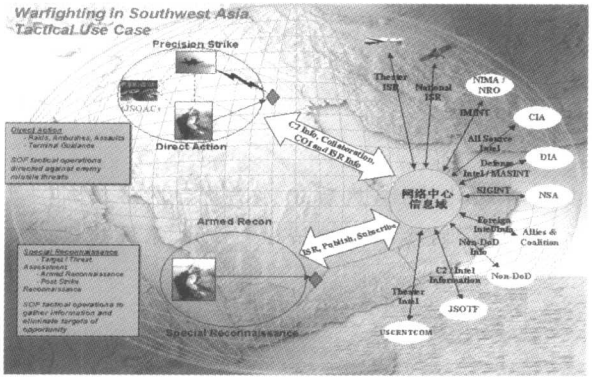

图 2 GIGv2.0 —Block4—高层作战概念图

我们可以看出全球信息栅格为网络中心战的实施提供了无所不在的通信、计算与安全等服务。而在所有的节点中,最引人注意的是名为"网络中心信息域"的这个节点。它是所有信息交换的另一端。所有的作战节点,无论是信息的生产者还是信息的使用者,抑或同为两者,都必须与网络中心信息域连接,可以说,网络中心信息域是战场的信息中心。事实上,与栅格中的节点不同,网络中心信息域是一个虚拟节点,它是全球信息栅格所提供的九类核心企业服务的集合。这九类服务包括企业系统管理服务、消息传递服务、仲裁服务、协同服务、用户帮助服务、信息保障和安全服务、存储服务与应用程序服务。

网络中心信息域的存在体现了网络中心战与平台中心战最根本的区别,即信息交换方式的转变。传统的平台中心环境中,信息生产者与信息用户之间直接关联,信息来源相对单一且固定,战斗人员、决策者,以及武器系统执行什么样的行动,完全依赖于其对应的信息源提供什么样的信息,可以说是信息的生成者主导着信息的内容与分配。而在 NCOW 环境中,所有使用信息技术的信息交换都是在栅格上进行的。信息生产者利用虚拟节点——网络中心信息域——的服务与设施,将信息发布到栅格中。而发布在栅格中的数据则在栅格中进行融合,并产生新的信息产品。用户可以使用搜索,或者订阅的方式从栅格中获取所需的、具有不同融合层次的信息,而无需关心所用信息的生产者是谁。可以说,在 NCOW 环境中,决定信息交换的是信息用户。这种以信息用户为主导的信息交换方式为权力前移的实现提供了基础。

2.2 NCOW 的企业体系结构

GIGv2.0 对于 NCOW 的支持最突出的就是体现在对网络中心信息域的描述。为了有助于说明,我们将图 1 与图 2 进行比较。作为原型体系结构,GIGv1.0 的作用是证明依照框架的体系结构描述方法对于体系结构集成的正确性与适用性。它描述的是为支持一支联合特种部队在西南亚执行的作战行动,美军现有的(As—Is)各种信息系统之间所要求的信息交换关系。在图 1 中,各种连线纵横复杂,节点之间的信息交换是一种直接关联的方式,即信息生产者与信息使用者之间点对点联系,其中每一个节点都可能与多个节点相连,而同样两个节点之间也可能存在着多种信息关联。对于信息的使用者和生产者来说,它们之间必须首先建立直接的连接才能够实现信息的流动。因此从图 1 上看,所有这些节点与连线似乎组成了一个复杂的网络,但是对于其中某一个节点来说,其发送或接收的信息并不是来源于一个网络,而是来自一个或几个固定的节点。而这正是 GIGv1.0 与 v2.0 区别的根本所在,因为在 GIGv1.0 中,执行作战与支持作战的环境并不是一个目标网络中心环境,而是美军现有的烟囱式信息环境。

相比之下,目标体系结构 GIGv2.0 中的网络中心信息域的提出,大大简化了这种错综复杂的信息交换关系,而代之以由全球信息栅格提供的九项核心企业服务所组成的虚拟节点。所有的信息都发布到网络中心信息域中,由它完成信息的收集、融合、处理与分发。无论是信息的使用者还是生产者,只需通过信息栅格从网络中心信息域中提拉或发布信息就行了。网络中心信息域的存在,使得只要是接入 GIG 的用户,其信息访问只会受到安全政策的限制。所有的信息发布与访问都是直接面向网络的,让网络作为信息交换的中心,而网络中心信息域则成为了 GIG 与所有接入用户的唯一的接口。在相应的 SV—1(系统接口,图 3)中,更加清楚地表示了这一点。

(下转第 11 页)

复杂网络理论对 C⁴ISR 系统建设的启示

罗 晨 李 渊 鲍广宇 刘晓明
（解放军理工大学指挥自动化学院）

摘 要 首先介绍了复杂网络涉及的重要参数及其统计特性，然后分析了复杂网络给新时期 C⁴ISR 系统建设所带来的各种挑战，最后讨论了将复杂网络理论应用于 C⁴ISR 系统建设的几点启示。

关键词 复杂网络，C⁴ISR，小世界，无尺度

0 引言

近年来的研究发现，许多现实系统都可以用一个复杂网络来描述，我们就生活在一个充满各种各样复杂网络的世界中，比如各种交通运输网，通信网，人际关系网等等。而近年来发生的一些重大网络事件，比如由于复杂电力网络的一系列级联反应所导致的北美地区的大停电事故，“爱虫”病毒在互联网上大肆传播所造成的一天十多亿美元的全球经济损失，让人们逐渐意识到复杂网络所发挥的不可估量的作用。

复杂网络同样存在于军事领域。计算机和互联网的发展在使社会形态由工业社会向信息社会转变的同时，也促使战争形态由机械化战争向信息化战争转变，由平台中心战向网络中心战转变。指挥自动化系统也由最初的 C² 扩展为 C⁴ISR，系统中所包括的指挥网、信息网、交战网、传感器网等多种网络结构越来越复杂，其间相互作用构成的复杂网络给 C⁴ISR 建设带来了前所未有的挑战。因此将复杂网络理论的研究成果应用于 C⁴ISR 系统的建设是有意义的。

1 复杂网络的重要参数

1.1 度分布

度分布是描述节点特征最简单的也是研究最多的概念。一个节点所拥有的度是该节点与其他节点相关联的边数，度是描述网络局部特性的基本参数。网络中并不是所有节点都具有相同的度，系统各节点度通常用度分布函数 $P(k)$ 来描述，它表示一个随机选取的节点的度为 k 的概率。度分布函数反映了网络系统的宏观统计特征。理论上利用度分布可以计算出其他表征全局特性参数的量化数值。

1.2 平均路径长度

平均路径长度是网络中所有节点之间的平均最短路径长度。在由 N 个节点组成的网络中，第 i 个节点到第 j 个节点的距离为：从节点 i 最少经过多少次连接到达节点 j，定义 $l_{\min}(i)=\frac{1}{N}\sum_{i=1}^{N}l(i,j)$。则平均最短路径为 $\bar{l}=\frac{1}{N}\sum_{i=1}^{N}l_{\min}(i)$。平均最短路径描述了节点对间的平均分离，同时也反映了网络的尺寸，因此常叫做网络直径。

1.3 集聚系数

集聚系数的概念起源于社会科学，比如，在一个人的朋友圈中，他的朋友中的两个很可能也是朋友。一个节点的集聚系数 C 是指在网络中与该节点相连的两个节点之间也彼此相连的条件概率。

给定节点 i，k_i 为节点 i 的度，也就是节点 i 有 k_i 个节点与它相连，这 k_i 个节点之间最多存在 $\frac{1}{2}k_i(k_i-1)$ 条边，则节点 i 的集聚系数可以定义为 $C(i)=\frac{2E(i)}{k_i(k_i-1)}$，其中 $E(i)$ 是这 k_i 个节点之间实际存在的边数。不难看出 $C(i)$ 是一个局域几何量，它只描述节点 i 附近的集聚系数。

而对于整个网络而言，网络的集聚系数就是所有节点集聚系数的平均数：$C=\frac{1}{N}\sum_{i=1}^{N}C(i)$。

2 复杂网络统计特性

网络的拓扑结构决定着网络的统计特性。Erdös 和 Re'nyi 在 1960 年提出随机网络模型,其节点度分布服从泊松分布;随机网络模型统治了将近 40 年,然而,上世纪末,随着计算机能力的飞速提高以及数据库的迅速膨胀,很多试验表明,现实世界的网络特征已不能用随机图进行较好的描述,这就促使人们打破边界条件,寻求新的模型。其中最典型的两类模型分别是 Watts 和 Strogatz 与 1998 年提出小世界模型(WS)以及 Baraba'si 和 Albert 与 1999 年提出的无尺度网络模型(BA)。实践证明,复杂网络大都具有小世界特性或无尺度特性。

2.1 小世界特性

小世界网络模型的构造过程如下:

① 开始于规则图形。初始有数目固定的 N 个节点,每个节点的度为 $d=2r$,构成一个规则的一维圆环。

② 随机化。以概率 p 随机地重新连接每一条边。这个过程中不能自身连接和重复连接,即重连后的边不能与原边重合,一对节点最多只能有一条边相连。整个过程没有改变节点的平均度。

从 0 至 1 选取不同的概率值 p,重连后的图变得越来越无序。如图 1 所示。

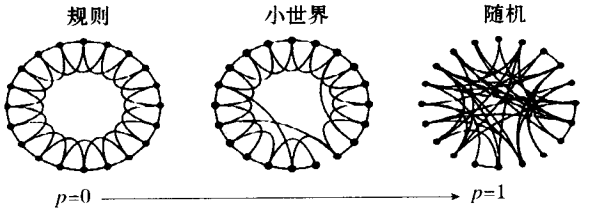

图 1 $N=20, k=4$ 时的 WS 模型

当 $p=1$ 时,重连后的网络几乎变成一个随机网络。而 p 在 0～1 之间时网络呈现小世界的特性,小世界模型具有较短的平均最短路径和较大的集聚系数。

2.2 无尺度特性

现实的一些复杂网络具有两个特征:① 具有开放性,并且它们是由新节点的不断加入而形成的;② 在产生新连接时,并不是像随机网络和小世界网络那样具有相同的概率。而是随着新节点的加入,网络不断增加,新的节点优先连接到有大量连接的节点上,综合这两点即是网络的无尺度特性。

BA 模型构造过程如下:

① 增长:开始于较少的节点数量(m_0),在每个时间间隔增添一个具有 $m(m \leqslant m_0)$ 的新节点,连接这个新节点到 m 个已经存在于系统中的节点上。

② 择优连接:在选择新节点的连接点时,新节点连接到节点 i 的概率取决于节点 i 的度数。

根据以上规则得到的无尺度网络模型节点度分布服从幂律分布,即 $P(k) \sim k^{-r}$,幂指数 $r=3$。

3 C⁴ISR 系统建设所面临的挑战

现代科学技术特别是计算机和网络的应用发展,给军队的建设模式带来了根本性的转变,同时也对 C⁴ISR 系统建设提出了更新更高的要求。一方面,极大地提高了 C⁴ISR 系统的指挥、控制、通信、情报等各方面工作的效率,使作战指挥发生了质的飞跃;另一方面,指挥自动化系统中所涉及到的指挥关系网,信息传输网,交战网等网络的规模日益庞大,结构也日益复杂,如何在如此复杂的网络中提供有效的手段使指挥自动化系统在作战中发挥最大的效能是当前 C⁴ISR 系统建设所面临的挑战。本文将着重从复杂性、可靠性和生存性三方面来讨论。

3.1 复杂性挑战

作战理论决定 C⁴ISR 系统的发展方向,网络中心战是近年美军提出的一种新的作战理论。1997 年 4 月,美国海军作战部部长约翰逊上将首次创造性的提出了以网络中心战理论牵引信息化建设的概念。2001 年 7 月美国国防部向国会正式提交了《网络中心战》报告。网络中心战利用信息网络把各种探测器、武器系统、指挥控制系统有机地联系在一起,在物理域将部队的各种作战力量和武器平台都安全可靠地网络化,实现无缝连接。因此网络中心战依赖于分布于全球各地的功能强大的网络,这些网络包括指挥关系网、信息传输网、交战网,这些网络为所有实体节点提供近乎实时的数据流,促进分散配置的各部队对作战信息的实时共享。因此,C⁴ISR 系统中网络的复杂性是前所未有的,如何应对复杂性带来的挑战,如