

# 基于复杂网络的军事通信网络建模与脆弱性分析

郭昊明<sup>1</sup>, 汪霜玲<sup>2,3</sup>, 燕雪峰<sup>1,4</sup>, 张科成<sup>2,3</sup>

1.南京航空航天大学 计算机科学与技术学院, 江苏 南京 211106;  
2.信息系统工程重点实验室, 江苏 南京 210007;  
3.中国电子科技集团有限公司 第二十八研究所, 江苏 南京 210007;  
4.软件新技术与产业化协同创新中心, 江苏 南京 210093

**摘要:**针对军事通信体系复杂性和网络化结构特点,基于复杂网络理论,引入中继通信实体(节点),通过分析装备实体间的通信关系,构建了军事通信网络结构模型。在此基础上,从网络概率重构模型和基于节点属性的级联失效传播模型角度出发,分析了军事通信网络的脆弱性。此外,给出了军事通信网络脆弱性的评价指标。通过仿真实验,验证了所提模型方法的有效性,为军事通信网络的分析建设提供了理论依据。

**关键词:**复杂网络;军事通信网络;脆弱性分析;网络重构;级联失效

中图分类号:TP393

文献标志码:A

文章编号:1000-2758(2024)06-1126-09

随着现代战争的快速发展,信息化和网络化已成为战争取胜的关键。军事通信网络在各战略体系间、各子系统间以及单个作战个体间发挥着关键作用,它能够实现战场信息实时、稳定传递与接收,为提升整体战斗能力提供基础支撑,并且具备高速、安全、可靠的特点<sup>[1-2]</sup>。然而,随着军事通信体系结构日益复杂化,网络故障可能导致连通性受损,进而影响关键信息的正常传输<sup>[3-5]</sup>。因此,军事通信网络的建模与脆弱性分析对于完善军事通信系统的理论体系具有重要的实践意义。

军事通信网络作为现代战争中的神经网络,承担着指挥控制、情报侦察、火力打击等重要任务。该网络由多个不同类型的节点组成,通过特定的拓扑结构进行作战指挥、通信联络与信息传输<sup>[6-7]</sup>。对军事通信网络的研究首先需要建立合适的网络结构模型,这是深入研究实际网络的基础。军事通信网络结构模型的建立或描述嵌入在军事通信网络其他相关研究中,这些研究包括网络抗毁性、生存性、连

通性和可靠性等<sup>[8-11]</sup>。杨芷柔等<sup>[12]</sup>以优化网络的鲁棒性为研究目标,提出了一种节点攻击策略下的军事通信网络结构优化方法,将侦察探测、火力打击和指挥控制实体抽象为军事通信网络的节点,并建立了相应的网络结构模型。刘同林等<sup>[13]</sup>考虑了体系中装备实体和各装备之间的通信关系,从而构建了军事通信网络图结构模型,从网络抗毁性、节点重要性以及通信链路重要性分析了军事通信网络的性能。此外,学者们还通过采用复杂网络中节点重要性<sup>[14]</sup>和链路重要性<sup>[15]</sup>的评估方法研究军事通信网络的性能。对于军事通信网络来说,可以从网络重构<sup>[16-17]</sup>和网络级联失效角度<sup>[18-19]</sup>度量性能。网络重构反映了当网络拓扑结构受损或部分节点/链路失效时,如何通过重新配置网络连接以确保通信的可靠性与稳定性;网络级联失效是指在军事通信网络中,当某些关键节点或链路发生故障时,这些故障可能会导致网络中其他节点或链路的级联失效,从而引发更广泛的通信中断或降级。

因此,本文在军事通信体系中引入中继通信实体,并通过分析装备实体之间的通信关系,构建军事通信网络结构模型,提出了基于概率重构的网络模型和基于节点属性的级联失效传播模型,并依据脆弱性指标对军事通信网络进行脆弱性分析。最后通过构建军事通信网络拓扑模型进行仿真实验,验证

收稿日期:2023-10-10

基金项目:国家自然科学基金重点项目(U2033202)与信息系统工程重点实验室开放基金(05220202)资助

作者简介:郭昊明(1995—),博士研究生

通信作者:燕雪峰(1975—),教授 e-mail: yxf@nuaa.edu.cn

了理论分析的结果。

## 1 军事通信网络建模

### 1.1 通信网络节点建模

军事通信网络作为作战网络的重要组成部分,通过不同节点之间传递信息来完成作战任务。军事通信网络由多种不同类型的节点组成。根据节点在作战体系中的作用和功能,可以分为侦察节点 O (observe)、指控节点 D (decide) 以及行动节点 A (act)。其中,侦察节点 O 通过侦察来实时关注战场信息,为上级指控节点提供信息支撑;指控节点 D

根据敌方信息进行分析、判断、决策和协同决策,为作战指挥提供重要依据;行动节点 A 具备执行作战任务的能力,包括独立作战、协同作战和联合火力打击等。假设通信网络包含中继通信节点 C (communication),特指的装备实体包括飞艇、卫星、高空无人机等,主要功能是实现各个节点之间的连接,确保通信畅通与信息传递的稳定性。综上所述,侦察节点、指控节点、行动节点和中继通信节点共同构成了完整的作战网络,并形成了一体化的军事通信网络,为作战行动提供了高效的支持和保障。军事通信网络中各节点类型、通信功能及作战功能的描述如表 1 所示。

表 1 军事通信网络节点类型

节点类型		符号	具体功能描述	实体
通信功能	作战网络			
中转信息	中继通信节点	C	实现信息的交互,完成 2 个节点之间的信息交流	飞艇、高空无人机
收集信息	侦察节点	O	通过侦察感知,收集战场的态势信息	侦察机、侦察卫星
使用信息	指控节点	D	通过侦察节点提供的信息,做出决策	指控中心
执行信息	行动节点	A	执行指控节点给出的指令,完成相关任务	打击中心

### 1.2 通信网络链路建模

在军事通信网络中,节点之间的紧密配合体现在信息的收集、中转、使用与执行效果上。整个过程大致可以划分为以下几种信息类型:态势流信息包括侦察节点将收集的信息上报给指控节点,侦察节点通过中继通信节点中转上报态势信息,以及侦察节点之间的信息交互共享等。指控流信息包括指控

节点之间的协同决策,指控节点通过中继节点中转信息实现协同决策,以及指控节点向行动节点下达指令等。状态流信息包括行动节点将战场作战信息上报给指控节点,或通过中继通信节点中转上报等。军事通信网络通过不同类型的信息流实现战场通信功能,军事通信网络节点之间的交互类型如表 2 所示。

表 2 通信网络节点的交互类型

功能	交互类型	功能描述	信息类型
上报态势信息	O-D	侦察节点将收集的战场数据和态势信息上传给指控节点	态势流
	O-C-D	侦察节点将收集的战场数据和态势信息通过中继通信节点中转传输给指控节点	
	O-O	侦察节点之间直接传输信息共享	
共享态势信息	C-C	中继通信节点之间的信息共享	态势流
	O-C-O	侦察节点之间通过中继通信节点传输信息	
共享决策信息	D-D	指控节点之间共享决策信息实现协同决策	指控流
	D-C-D	指控节点之间通过中继通信节点传输决策信息	
行动信息分配	D-A	指控节点将指控信息下达传输给行动节点	指控流
	D-C-A	指控节点将指控信息通过中继通信节点传输给行动节点	
交战信息反馈	A-D	行动节点将战场毁伤态势信息上报传输给指控节点	状态流
	A-A	行动节点之间的信息协同交互	
	A-C-D	行动节点将战场毁伤态势信息通过中继通信节点传输给指控节点	

### 1.3 军事通信网络框架结构

基于观察、判断、决策、行动 (observe, orient,

decide, act, OODA) 作战循环理论<sup>[20]</sup>,本节给出了军事通信网络框架结构。如图 1 所示,假设军事通信网络是由指挥控制网、传感网、行动网和中继通信网

构成的,其中,中继通信网可以把指挥控制网、传感网和行动网有效地连接起来,以支持整个作战体系的通信和协调。传感网是负责收集战场信息的网络,包括各种传感器、侦察设备和监视系统。它们能够观察战场环境,收集敌我双方的动态信息,为指挥控制网提供实时的情报支持。指挥控制网是负责决策制定和命令下达的网络。它接收来自传感网的信息,进行分析和判断,制定作战计划和指令,然后通过中继通信网下达给行动网执行。行动网是负责执行指挥控制网下达指令的网络。它包括各种作战单位、武器系统和支援设施,负责根据指挥控制网的命令开展实际的军事行动。中继通信网是负责连接指挥控制网、传感网和行动网的网络。它提供稳定可靠的通信链路,确保信息能够及时准确地在各个网之间传递,支持整个作战体系的通信和协调需求。

侦察节点、指控节点、行动节点和中继通信节点构成节点集合:  $V = \{v_o, v_D, v_A, v_C\}$ 。根据节点交互类型构成连边集合:  $E = \{e_1, e_2, \dots, e_n\}$ 。军事通信网络总节点数  $N = N_o + N_D + N_A + N_C$ 。其中,  $N_o, N_D, N_A, N_C$  分别表示侦察节点、指控节点、行动节点和中继通信节点的数量。假设军事通信网络中节点之间连边的连接概率为:  $P = (P_{oo}, P_{DD}, P_{AA}, P_{CC}, P_{oD}, P_{DA}, P_{oC}, P_{CD}, P_{CA})$ 。  $P_{oo}, P_{DD}, P_{AA}, P_{CC}$  分别代表侦察节点之间、指控节点之间、行动节点之间、中继通信节点之间的连接概率,  $P_{oD}$  代表侦察节点与指控节点的连接概率,  $P_{DA}$  代表指控节点和行动节点之间的连接概率,  $P_{oC}$  代表侦察节点和中继通信节点之间的连接概率,  $P_{CD}$  代表中继通信节点和指控节点之间的连接概率,  $P_{CA}$  代表中继通信节点和行动节点之间的连接概率。

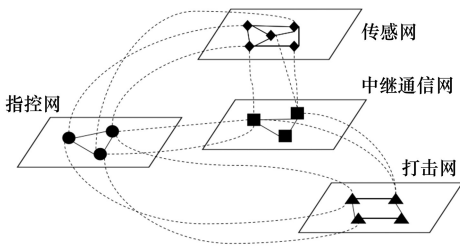


图 1 军事通信网络的简单框架结构

## 2 军事通信网络脆弱性度量模型

### 2.1 基于概率重构的模型

军事通信网络的重要节点和链路是敌方攻击的

主要目标。在实际作战中,受攻击的节点可能会出现故障或失效,导致与之相连的链路失效,进而削弱网络的通信能力。为保证作战体系的通信不受影响,受损的通信网络会进行动态重组,增加新的连接关系以维持整体通信能力。然而,这种重构能力有限,当失效节点达到一定比例时,网络将无法通过动态重组恢复功能,此时网络达到了脆弱性临界水平。本文在军事通信网络脆弱性分析中,考虑网络概率重构过程,给出了动态重构策略及概率重构条件。

军事通信网络概率重构策略:假设  $t$  时刻,军事通信网络中的节点  $v_x^i$  被攻击而失效,导致与节点  $v_x^i$  连接的所有连边都失效,造成了军事通信网络通信能力降低。假设在  $t + \Delta t$  时刻,网络中存在与失效节点  $v_x^i$  同类型的节点  $v_x^j, i \neq j$ ,那么从同类型节点中随机选择某一节点  $v_x^j$ ,判断节点  $v_x^j$  是否具有替代节点  $v_x^i$  能力。这里定义 2 个判定条件:

条件 1 节点  $v_x^i$  在失效前和节点  $v_x^j$  之间存在连边,也就是说节点之间的可以实现信息交互。

条件 2 节点  $v_x^j$  和节点  $v_x^i$  的度值比需满足  $p = k(v_x^j)/k(v_x^i)$  条件,本文假设  $0 < p \leq 1$ 。

当节点  $v_x^j$  满足以上条件时,代表节点  $v_x^j$  可以替代  $v_x^i$  完成其功能,即把和  $v_x^i$  相连的网络边与  $v_x^j$  相连。当  $v_x^i$  与  $v_x^j$  之间存在边时,在重构过程中,不考虑增加新的边。根据以上分析,下面给出一个军事通信网络概率重构过程案例并进行简要分析。

图 2 简要描述了军事通信网络节点失效以及概率动态重构的过程。网络中包括 3 个侦察节点,3 个

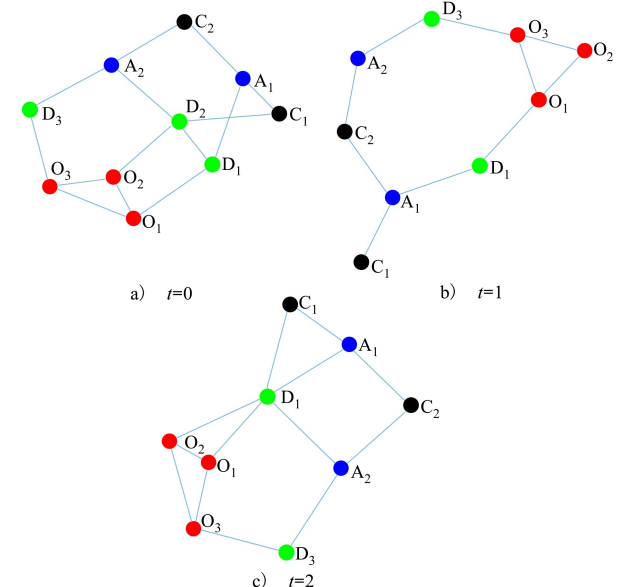


图 2 军事通信网络概率重构过程案例

指控节点,2个行动节点,2个中继通信节点。其中, $t=0$ 时刻为初始军事通信网络。当 $t=1$ 时,军事通信网络中的指控节点 $D_2$ 受到攻击,与 $D_2$ 连接的所有边都失效。 $t=2$ 时刻,与节点 $D_2$ 的同类型节点有节点 $D_1$ 和节点 $D_3$ ;仅有节点 $D_1$ 和节点 $D_2$ 有连边,且 $p = k(v_{D_1})/k(v_{D_2}) = 0.75$ ;因此,节点 $D_1$ 满足概率重构的条件1和条件2;此时,军事通信网络进行动态重构,选取节点 $D_1$ 进行替代,将节点 $D_1$ 与 $D_2$ 连接的失效边都连接上,实现网络的动态重组,动态重构后的网络如 $t=2$ 时刻所示。

## 2.2 基于节点属性的级联失效模型

在网络中,一个节点或者少数几个节点的故障,可能会导致与故障节点相连接的其他节点发生故障,从而发生连锁效应,最终导致网络瘫痪,这种现象称为级联失效。军事通信网络中的节点类型不同导致节点属性差异很大,本节基于军事通信网络建立级联失效传播模型,分析节点的初始负载和节点容量对军事通信网络结构脆弱性的影响。为了构建符合军事通信网络的级联失效模型,结合节点属性,建立如下模型。

初始负载的定义:为了体现节点属性对于节点负载的影响,定义节点的初始负载为节点的度与其同类型邻居节点度的总和乘积,表示为

$$L_i^0 = \left( k_x^i \sum_{m \in \Gamma_i} k_x^m \right)^\alpha, i = 1, 2, \dots, N, \quad (1)$$

式中: $L_i^0$ 表示节点 $v_x^i$ 的初始负载; $k_x^i$ 为节点 $v_x^i$ 的度; $\Gamma_i$ 为节点 $v_x^i$ 的同类型邻居节点的集合; $k_x^m$ 是同类型邻居节点 $v_x^m$ 的度; $\alpha$ 是一个可调参数,控制初始负载的强度; $N$ 是网络中的节点总数。

节点容量的定义:ML模型<sup>[21]</sup>被大多数研究所采用,节点容量体现了网络中节点可以承受的最大负载。在保证节点容量与节点初始负载呈正比的前提下,由于本文的节点具有不同类型,节点容量会随节点类型的不同而变化,为体现这一特性,引入属性权重 $\gamma_x$ ,建立的节点容量模型为

$$C_i = (1 + \beta^{\gamma_x}) L_i^0 \quad i = 1, 2, \dots, N \quad (2)$$

式中: $C_i$ 表示节点 $v_x^i$ 的容量; $\beta$ 是可调参数,且 $\beta > 0$ ; $\gamma_x$ 是随着节点类型变化的相对权重; $x$ 表示节点类型, $0 < \gamma_x < 1$ ,且 $\gamma_0 + \gamma_D + \gamma_C + \gamma_A = 1$ 。 $L_i^0$ 是节点 $v_x^i$ 的初始负载, $N$ 是网络中的节点总数。

## 2.3 脆弱性评价指标

评价军事通信网络在遭受破坏事件后的脆弱程度的一种直观方法是通过移除网络中的节点和连边

来观察网络最终的连通情况。删除军事通信网络中的不同节点,会对网络的连通性产生不同程度影响。例如,删除通信网络中度相对较小的侦察节点,不会对网络连通性有明显影响,而移除通信网络中度相对较大的指控节点,则可能导致网络的连通性明显降低。根据文献[12]的军事通信网络性能度量指标,本文通过模拟移除网络节点来模拟破坏事件的发生,因此可以通过比较网络中断前后连通子图大小的变化来表征网络的脆弱性

$$F_N = \frac{N'}{N} \quad (3)$$

式中: $F_N$ 代表网络连通性相对大小,军事通信网络中节点初始总量为 $N$ ,攻击事件后网络的最大连通子图包含的节点数量为 $N'$ 。军事通信网络在遭受破坏事件后连通性受到的影响程度体现出网络的脆弱性。即 $F_N$ 越小表示网络的脆弱性越大,反之表示网络的脆弱性越小。

## 3 仿真结果与分析

为验证所提模型的有效性,选取某作战编队的通信网络为研究背景。通信网络中的节点总数 $N=70$ ,其中包括侦察节点 $N_0=20$ ,指控节点 $N_D=15$ ,行动节点 $N_A=10$ ,中继通信节点 $N_C=25$ 。为了便于分析,假设同类型节点之间的连接概率为0.5,即 $P_{00}=P_{DD}=P_{AA}=P_{CC}=0.5$ ,不同类型节点之间的连接概率为0.4,即 $P_{0D}=P_{DA}=P_{0C}=P_{CD}=P_{CA}=0.4$ 。基于以上分析,可以生成节点总数为70的通信网络,拓扑结构如图3所示。

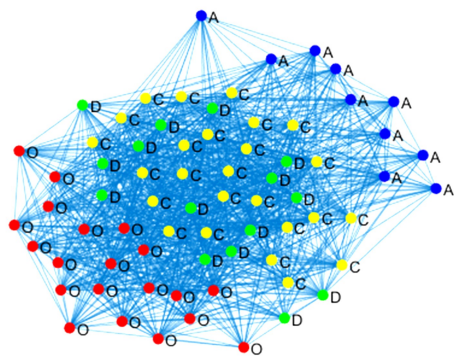


图3 节点总数为70的军事通信网络拓扑结构

### 3.1 基于概率重构的网络脆弱性分析

本节根据图4所示的基于概率重构算法的网络

脆弱性分析流程,分别对蓄意攻击策略和随机攻击策略下,有重构网络与无重构网络的脆弱性进行分析。蓄意攻击策略是依次找到网络中度值最大的节点进行攻击;随机攻击策略则是随机选取网络中的节点进行攻击。

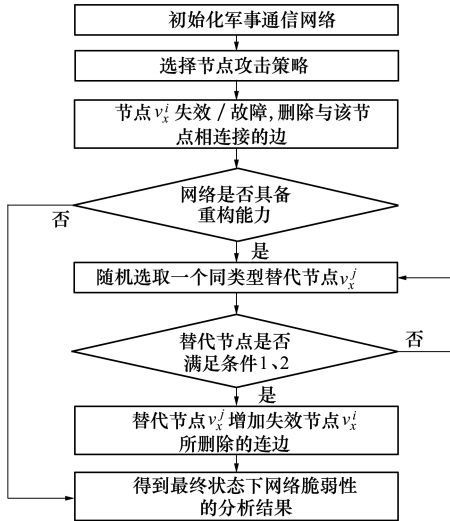


图 4 基于概率重构算法的网络脆弱性分析流程

考虑蓄意攻击策略下,网络在动态重构和无重构情况下的脆弱性变化。假设蓄意攻击策略为基于节点度值大小的攻击原则,即根据节点度值由大到小进行攻击。图 5 给出了基于节点度大小蓄意攻击下动态重构和无重构的脆弱性分析结果,其中,纵坐标为网络的连通性,  $F_N$  越大代表网络的脆弱性越小,横坐标为网络节点的移出比例。在临界点  $F_N = 0$ ,即网络连通性相对大小为 0 之前,移出节点的比例相同时,动态重构通信网络的连通性相对大小明显高于无重构的通信网络,也就是说,动态重构通信网络的脆弱性低于无重构通信网络。

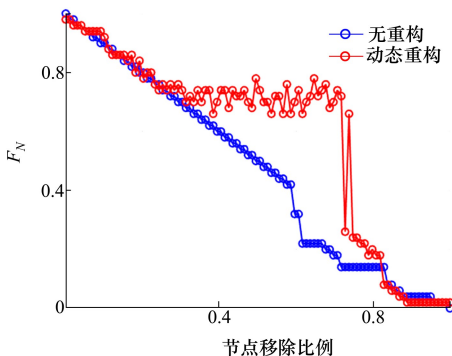


图 5 蓄意攻击下动态重构和无重构的脆弱性结果

考虑随机攻击策略下,网络在动态重构和无重构情况下的脆弱性变化。图 6 给出了军事通信网络在随机攻击策略下动态重构和无重构的脆弱性结果。由图可知,当移出节点的比例相同时,动态重构的连通性明显高于无重构网络。这表明在随机攻击策略下,动态重构网络的脆弱性低于无重构通信网络。这充分说明了动态重构过程能进一步降低通信网络的脆弱性。

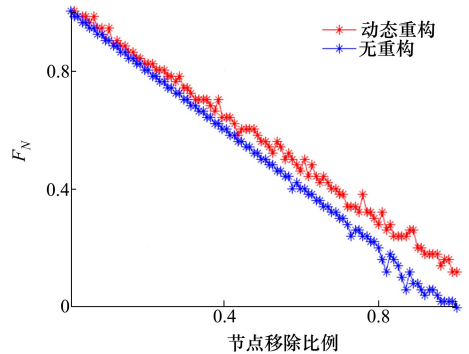


图 6 随机攻击下动态重构和无重构的脆弱性结果

综上所述,在相同攻击策略下,动态重构的军事通信网络脆弱性低于无重构军事通信网络的脆弱性。

### 3.2 级联失效传播下的脆弱性分析

本节根据图 7 基于级联失效传播算法的网络脆弱性分析流程,分别针对调节参数  $\alpha, \beta$ , 权重系数  $\gamma_x$  以及不同攻击策略展开军事通信网络脆弱性分析。

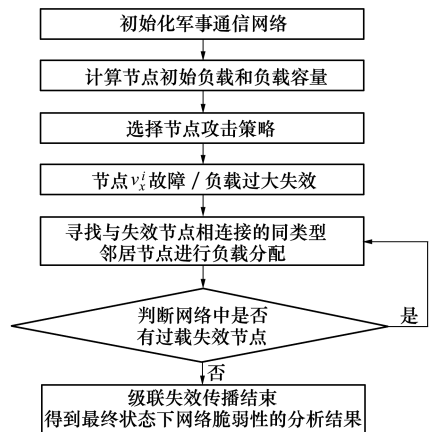


图 7 基于级联失效传播的网络脆弱性分析流程

#### 3.2.1 不同参数对网络脆弱性的影响

考虑调节参数  $\alpha$  对网络脆弱性的影响,假设节点失效后的负载分配策略为平均分配,令调节参数  $\beta = 1$ , 权重系数  $\gamma_x = 0.25$ 。对调节参数  $\alpha$  取不同值,

考虑随机攻击策略下,网络在动态重构和无重

结果如图 8 所示。

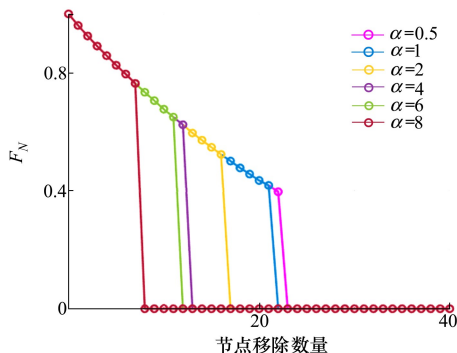


图 8 不同节点初始负载对脆弱性的影响

从图 8 可以观察到当参数  $\alpha$  的值增大时,即节点的初始负载增大时,网络的脆弱性也随之增加。具体而言,移除很少的节点网络的连通性就会显著下降,导致整个网络的相对大小趋近于零。这种情况下,网络处于崩溃状态,意味着即使对网络进行微小扰动,也能够导致系统彻底瘫痪。因此,随着调节参数  $\alpha$  的越大,网络的脆弱性也越大。

考虑调节参数  $\beta$  对网络脆弱性的影响,采用的失效节点的负载分配策略为平均分配,调节参数  $\alpha = 0.5$ ,权重系数  $\gamma_x = 0.25$ 。对调节参数  $\beta$  取不同值,结果如图 9 所示。

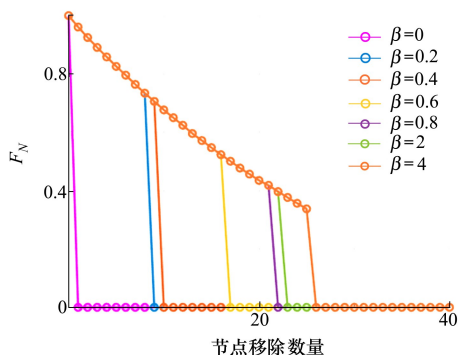


图 9 不同节点容量对脆弱性的影响

根据图 9 可知,节点容量随着参数  $\beta$  的增大而增加。节点容量的增加对网络的连通性产生积极影响。意味着网络的脆弱性逐渐降低,即网络更具抗干扰和抗攻击能力,更不容易崩溃。较大的节点容量使得网络能够承载更多的负载和数据传输,并能够更好地适应流量和负荷的变化。然而,需要注意的是,尽管节点容量可以随参数  $\beta$  的增大而增加,但受到物理和资源限制,节点容量无法无限增大。因此,即使网络的脆弱性降低,仍需合理规划和管理节

点容量,以确保网络能够在可接受的范围内运行,并满足用户需求。

考虑权重系数  $\gamma_x$  对网络脆弱性的影响,选取中继通信节点作为攻击节点,分析权重系数  $\gamma_c$  对网络脆弱性的影响,令其他调节参数  $\alpha = 0.5, \beta = 2$ 。对权重系数  $\gamma_x$  取不同值,结果如图 10 所示。

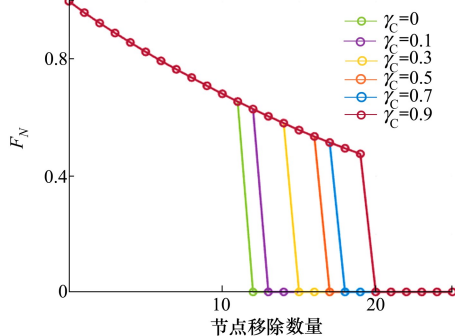


图 10 不同节点权重  $\gamma_c$  对脆弱性的影响

由图 10 可知,中继通信节点的权重系数  $\gamma_c$  越大,节点的容量也越大。这意味着中继通信节点具有更大的负载承载能力和传输容量。节点容量的增加使得网络的脆弱性降低,网络更加稳定。

### 3.2.2 不同攻击策略对网络脆弱性的影响

考虑不同攻击策略对于级联失效传播网络脆弱性的影响,采用的失效节点负载分配策略为平均分配策略。令调节参数  $\alpha = 0.2, \beta = 2$ ,权重系数  $\gamma_x = 0.25$ ,分析了基于节点度排序的攻击策略、随机攻击策略和基于节点介数的攻击策略对于级联失效传播网络脆弱性的影响,如图 11 所示。

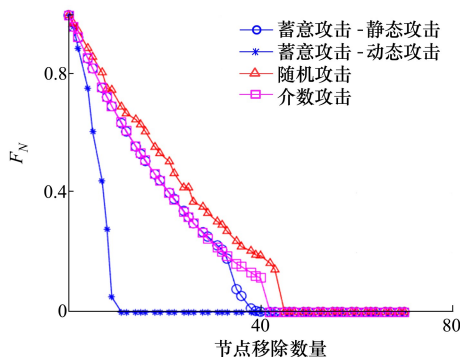


图 11 不同攻击策略下的脆弱性对比图

特别说明,基于节点度排序的攻击策略分为:按照初始网络中节点度排序进行攻击、每次攻击后重新评估当前网络的度最大节点进行攻击,这里简称为蓄意攻击的静态攻击策略和动态攻击策略。

从图 11 可以看出,在 4 种攻击策略中,随着移除节点数量的增加,网络的连通性呈现下降趋势。其中,在移除相同数量节点条件下,随机攻击策略导致网络连通性下降最慢,这表明随机攻击策略无法准确识别网络的脆弱性环节。蓄意攻击-动态攻击策略使网络连通性下降最快,表明该策略能够准确识别网络的脆弱环节,仅需移除少量节点便可使网络损伤达到最大效果,即网络进入崩溃状态。

## 4 结 论

在信息化、网络化战争环境下,军事通信网络作为信息的载体,具有举足轻重的作用。本文基于复杂网络理论,通过引入中继通信实体(节点)构建了军事通信网络结构模型。并从网络概率重构和基于

节点属性的级联失效传播 2 个角度分析了网络的脆弱性。最后,选取某作战编队的通信网络为研究背景进行仿真实验。实验结果表明:动态重构过程可以有效降低军事通信网络的脆弱性。网络节点的初始负载和容量对网络脆弱性有显著影响,基于节点类型变化的相对权重系数  $\gamma_x$  越大,网络的脆弱性越低。在级联失效传播模型中,不同攻击策略对网络脆弱性的影响存在差异。蓄意攻击-动态攻击策略能够准确识别网络的脆弱环节,对网络连通性的破坏最严重。

本文研究有助于深入了解军事通信网络的结构模型及通信节点之间的交互关系。通过建立概率重构模型和基于节点属性的级联失效传播模型,本研究为体系作战条件下军事通信网络脆弱性的分析提供了依据。

## 参考文献:

- [1] CHEN G, SUN P, ZHANG J. Repair strategy of military communication network based on discrete artificial bee colony algorithm [J]. *IEEE Access*, 2020, 8: 73051-73060
- [2] LI G J, HE G J, ZHENG M F, et al. Uncertain sensor-weapon-target allocation problem based on uncertainty theory [J]. *Symmetry*, 2023, 15(1): 176
- [3] GAO X, LI K Q, CHEN B. Invulnerability measure of a military heterogeneous network based on network structure entropy [J]. *IEEE Access*, 2017, 6: 6700-6708
- [4] SONG X, SHI W, TAN G, et al. Multi-level tolerance opinion dynamics in military command and control networks [J]. *Physica A Statistical Mechanics and Its Applications*, 2015, 437(1): 322-332
- [5] 苏臻, 高超, 李向华. 节点中心性对复杂网络传播模式的影响分析 [J]. *物理学报*, 2017, 66(12): 12  
SU Zhen, GAO Chao, LI Xianghua. Analysis of the effect of node centrality on diffusion mode in complex networks [J]. *Acta Physica Sinica*, 2017, 66(12): 12 (in Chinese)
- [6] YU M, SHANG W P, CHEN Z G. Exponential synchronization for second-order nodes in complex dynamical network with communication time delays and switching topologies [J]. *Journal of Control Science & Engineering*, 2017, 2017(1): 1-10
- [7] 陈静, 田晓杰, 曾兴善, 等. 基于复杂网络的军事通信建模及关键节点评估 [J]. *指挥控制与仿真*, 2021, 43(5): 55-59  
CHEN Jing, TIAN Xiaojie, ZENG Xingshan, et al. Military communication modeling and critical node evaluation based on complex network [J]. *Command Control & Simulation*, 2021, 43(5): 55-59 (in Chinese)
- [8] 孙昱, 姚佩阳, 申健, 等. 基于信息流的军事通信网络抗毁性优化设计 [J]. *华中科技大学学报*, 2016, 44(12): 114-120  
SUN Yu, YAO Peiyang, SHEN Jian, et al. Military communication network design for invulnerability optimization based on information flow [J]. *Journal of Huazhong University of Science and Technology*, 2016, 44(12): 114-120 (in Chinese)
- [9] 陈冠宇, 孙鹏, 张杰勇, 等. 军事通信网络修复策略 [J]. *浙江大学学报*, 2019, 53(8): 1536-1545  
CHEN Guanyu, SUN Peng, ZHANG Jieyong, et al. Repair strategy of military communication network [J]. *Journal of Zhejiang University*, 2019, 53(8): 1536-1545 (in Chinese)
- [10] 杨志才, 裘杭萍, 权冀川, 等. 基于网络流路径模型的军事通信网可靠性分析 [J]. *计算机工程*, 2015, 41(5): 125-129  
YANG Zhicai, QIU Hangping, QUAN Jichuan, et al. Reliability analysis of military communication network based on network

- flow path model [J]. *Computer Engineering*, 2015, 41(5): 125-129 (in Chinese)
- [11] 王智源, 丁泽中, 胡广水. 军事通信网络拓扑结构抗毁性仿真[J]. *计算机系统应用*, 2010, 19(12): 109-113  
WANG Zhiyuan, DING Zezhong, HU Guangshui, et al. Invulnerability simulation of military communication networks topology [J]. *Computer Systems & Applications*, 2010, 19(12): 109-113 (in Chinese)
- [12] 杨芷柔, 张虎, 刘静, 等. 节点攻击策略下的军事通信网络结构优化算法[J]. *系统工程与电子技术*, 2021, 43(7): 1848-1855  
YANG Zhirou, ZHANG Hu, LIU Jing, et al. Optimization algorithm of military communication network structure under node attack strategy[J]. *Systems Engineering and Electronics*, 2021, 43(7): 1848-1855 (in Chinese)
- [13] 刘同林, 杨芷柔, 张虎, 等. 基于复杂网络的军事通信网络建模与性能分析[J]. *系统工程与电子技术*, 2020, 42(12): 2892-2898  
LIU Tonglin, YANG Zhirou, ZHANG Hu, et al. Modeling and performance analysis of military communication network based on complex network[J]. *Systems Engineering and Electronics*, 2020, 42(12): 2892-2898 (in Chinese)
- [14] 阿地力·海里力, 吾斯曼·玉山. 基于布谷鸟算法的无线通信网络节点故障定位方法[J]. *长江信息通信*, 2023, 36(9): 183-185  
ADILI Hailili, WUSIMAN Yushan. Node fault location method of wireless communication network based on cuckoo search algorithm [J]. *Yangtze River Information and Communication*, 2023, 36(9): 183-185 (in Chinese)
- [15] 李鹏, 王世林, 陈光武, 等. 基于改进的局部结构熵复杂网络重要节点挖掘[J]. *计算机应用*, 2023, 43(4): 1109-1114  
LI Peng, WANG Shilin, CEHN Guangwu, et al. Key node mining in complex network based on improved local structural entropy [J]. *Journal of Computer Applications*, 2023, 43(4): 1109-1114 (in Chinese)
- [16] 孙利娜, 陈永禄, 陈志伟. 基于杀伤链的动态重构作战网络抗毁性分析[J]. *火力与指挥控制*, 2023, 48(2): 12-18  
SUN Lina, CHEN Yonglu, CHEN Zhiwei. Invulnerability analysis of dynamic reconfiguration combat network based on kill chain [J]. *Fire Control & Command Control*, 2023, 48(2): 12-18 (in Chinese)
- [17] 陈晓楠, 胡建敏, 池本亮, 等. 复杂作战网络体系博弈与重构方法[J]. *兵工学报*, 2021, 42(5): 1111-1120  
CHEN Xiaonan, HU Jianmin, CHI Benliang, et al. Game and reconfiguration method of complex combat network system [J]. *Acta Armamentarii*, 2021, 42(5): 1111-1120 (in Chinese)
- [18] 郑长江, 陶童统, 陈志超. 基于流量可调重分配的级联失效模型[J]. *吉林大学学报*, 2023, 6: 1-9  
ZHENG Changjiang, TAO Tongtong, CHEN Zhichao. Cascading failure model based on flow adjustable redistribution [J]. *Journal of Jilin University*, 2023, 6: 1-9 (in Chinese)
- [19] 孔芝, 袁航, 王立夫, 等. 节点分类及失效对网络能控性的影响[J]. *自动化学报*, 2022, 48(4): 1048-1059  
KONG Zhi, YUAN Hang, WANG Lifu, et al. Node classification and the influence of node failure on network controllability [J]. *Acta Automatica Sinica*, 2022, 48(4): 1048-1059 (in Chinese)
- [20] MOON T, KRUZINS E, CALBERT G. Analyzing the OODA cycle [J]. *Phalanx*, 2002, 35(2): 9-35
- [21] MOTTER A E, LAI Y C. Cascade-based attacks on complex networks [J]. *Physical Review E*, 2002, 66(6): 065102

# Modeling and vulnerability analysis of military communication network based on complex network

GUO Haoming<sup>1</sup>, WANG Shuangling<sup>2,3</sup>, YAN Xuefeng<sup>1,4</sup>, ZHANG Kecheng<sup>2,3</sup>

- 1.School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China;
- 2.Key Laboratory of Information Systems Engineering, Nanjing 210007, China;
- 3.The 28th Research Institute, China Electronics Technology Group Corporation, Nanjing 210007, China;
- 4.Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing 210093, China

**Abstract:** Aiming at the complexity of military communication system and the characteristics of network structure, based on the complex network theory, the relay communication entity (node) is introduced, and the communication relationship between equipment entities is analyzed, the military communication network structure model is constructed. On this basis, the vulnerability of military communication network is analyzed from two perspectives: the network probability reconstruction model and the cascading failure propagation model based on node attributes. In addition, the evaluation index of military communication network vulnerability is given. Finally, the effectiveness of the proposed model method is verified by simulation experiments, which provides a theoretical basis for the analysis and construction of military communication network.

**Keywords:** complex network; military communication network; vulnerability analysis; network reconstruction; cascading failures

**引用格式:** 郭昊明, 汪霜玲, 燕雪峰, 等. 基于复杂网络的军事通信网络建模与脆弱性分析[J]. 西北工业大学学报, 2024, 42(6): 1126-1134

GUO Haoming, WANG Shuangling, YAN Xuefeng, et al. Modeling and vulnerability analysis of military communication network based on complex network[J]. *Journal of Northwestern Polytechnical University*, 2024, 42(6): 1126-1134 (in Chinese)