文章编号：1000-3673（2026）01-0028-11 中图分类号：TM 721 文献标志码：A 学科代码：470·40

网络攻击下的综合能源信息物理系统的熵态建模与状态分析

刘佳委[1]，王丹[1,2]，李宜哲[1]，贾宏杰[1,2]，周天烁[1]，张帅[1]，程颢[1]
（1．智能配用电装备与系统全国重点实验室(天津大学)，天津市 南开区 300072；
2．天津市智慧能源与信息技术重点实验室(天津大学)，天津市 南开区 300072）

Entropy State Modeling and State Analysis of Integrated Energy Cyber-physical Systems Under Cyber Attacks

LIU Jiawei[1], WANG Dan[1,2], LI Yizhe[1], JIA Hongjie[1,2], ZHOU Tianshuo[1], ZHANG Shuai[1], CHENG Hao[1]
(1. National Key Laboratory of Intelligent Power Distribution and Utilization Equipment and System (Tianjin University), Nankai District, Tianjin 300072, China;
2. Key Laboratory of Smart Energy & Information Technology of Tianjin Municipality (Tianjin University), Nankai District, Tianjin 300072, China)

ABSTRACT: The integrated energy information physical system plays a vital role in the modern energy network, and enhancing its ability to withstand cyberattacks is crucial to ensure the reliability and security of the energy supply. Based on the law of entropy increase, this paper presents an entropy modeling method for the integrated energy information physical system under network attack. Firstly, the physical information flow coupling calculation model of the integrated energy information physical system is established. Then, a calculation model for information attack and a system disturbed by a network attack is constructed, and an evaluation index for the physical impact of network attacks based on power flow entropy is proposed. Finally, the influence of different types of information and physical attack modes on the entropy distribution of the integrated energy information physical system is analyzed through a numerical example, which provides a tool for quantifying the unavailability of energy after the attack, enriching the entropy state theory of the traditional integrated energy system, and providing a new perspective and method for the security protection of the integrated energy information physical system in the future.

KEY WORDS: integrated energy cyber-physical system; entropy state model; thermodynamic entropy; information entropy; cyber-attacks

摘要：综合能源信息物理系统在现代能源网络中扮演着至关重要的角色，增强其抵御网络攻击的能力对保障能源供应的可靠性和安全性至关重要。文章针对综合能源信息物理系统在网络攻击下的具体特性变化，基于物理学熵增定律提出了一种信息物理系统在受到网络攻击下的熵态建模方法。首先建立了综合能源信息物理系统的物理-信息流耦合计算模型；然后，构建了信息攻击以及系统受网络攻击扰动的信息等效热力学熵增计算模型，并针对网络攻击对系统的物理影响，提出了基于潮流熵的网络攻击物理影响评估指标；最后，通过算例分析了不同种类信息及物理攻击方式对综合能源信息物理系统熵态分布的影响，为量化系统受到攻击后能量的不可用性提供了工具，丰富了传统综合能源系统的熵态理论，同时为未来综合能源信息物理系统的安全防护提供了新的视角和方法。

关键词：综合能源信息物理系统；熵态模型；热力学熵；信息熵；网络攻击

DOI：10.13335/j.1000-3673.pst.2025.0492

0 引言

综合能源系统(integrated energy system，IES)通过电、气、冷、热等多种形式能源的协同互补，提高了能源的综合利用效率，如今受到广泛关注。随着能源互联网的发展，IES 中通信设施建设不断完善，能源网络时刻依赖一个强大的信息系统，以实现对其运行状态的态势感知与精准控制[1-2]。因此，IES 演变成典型的信息物理系统(cyber physical system，CPS)[3-4]——综合能源信息物理系统(integrated energy cyber physical system，IECPS)。

与传统仅针对信息领域(如互联网)的网络攻击不同，针对信息-物理耦合系统的网络攻击不仅限于

基金项目：国家重点研发计划项目(2023YFB2407300)。
Project Supported by National Key Research & Development Program of China (2023YFB2407300).

破解或窃取保密信息，其往往更注重破坏物理系统的稳定运行，造成大规模能量供应中断[5-6]。

为应对网络攻击给信息物理耦合系统稳定运行带来的不良影响，部分学者已陆续开展针对信息-物理耦合系统中信息攻击的研究，研究对象主要包括虚假数据注入攻击(false data injection attack，FDIA)、拒绝服务攻击(denial of service attack，DoSA)等[7]。文献[8]研究了电力信息物理耦合系统数据传输场景和虚假数据注入形式，分析了新型电力系统多样化智能终端设备攻击的各种后果。文献[9]建立了电网负荷削减算法的脆弱性分析模型，证明了 DoSA 会阻碍网络失稳状态下的负荷削减行为，从而影响系统的稳定恢复过程。总的来说，信息物理耦合系统在受到信息或物理攻击后，均会导致部分能量不可被利用，即出现能量退化现象。上述研究多聚焦于单一能源形式的信息物理耦合系统，且研究对象也局限于信息攻击机理，或攻击对信息和能源系统的破坏程度[10]。然而，对于攻击导致的能量退化现象，信息和能源领域的研究方向存在一定的割裂，且缺乏统一的指标来精确量化由信息、物理攻击分别导致系统能量退化的程度。

目前，已有学者对综合能源系统的能量不可用性进行了量化分析。在 IES 中，能量的产生、传输、转换、消费等过程是“熵增”过程[11]。文献[12]提出了面向源荷不确定性的信息学等效热力学熵增计算方法，实现了能量与信息层面熵增的统一分析，为量化信息对能源过程的影响提供了有利工具。而“IES 熵态”[13]则统一量化了 IES 中由于不同品质能量之间的转换，以及在高比例可再生能源集成背景下源荷不确定性导致的能量退化程度。文献[14]在熵态理论的基础上，考虑能源站熵增流的转化与分配机制，建立了基于顺序求解和联立求解的 IES 熵态计算模型，实现了熵态计算从递推运算向线性方程求解的转变。

针对现有信息物理耦合系统网络攻击研究的不足，在已有熵态理论研究的基础上，本文中网络攻击划分为物理攻击、信息攻击以及信息-物理协同攻击 3 种类型，提出了网络攻击下 IECPS 的熵态建模与网络攻击对系统物理影响的分析方法，该方法在考虑网络攻击给能源系统造成实际物理层面影响的基础上，建立了网络攻击的信息等效热力学熵增模型及其物理影响的评估指标，既统一刻画了传统源荷不确定性、网络攻击导致能量的退化程度，又量化描述了攻击发生后系统节点和支路能量供应的破坏情况，可以分别明确二者对系统能量退化的影响程度。首先，建立了信息-能量流耦合计算模型，明确了能源网络与信息网络的相互作用关系；其次，建立了信息攻击的熵态计算模型，明确了基于攻击图的信息网络状态节点遭受信息攻击的概率计算方法，同时考虑网络攻击成功概率中所蕴含的不确定性，提出了信息攻击的熵增计算方法；再次，为统一量化分析 IES 信息物理耦合系统在受到信息、物理组合攻击后，系统物理层面的能量不可用程度，提出了基于潮流熵的网络攻击物理影响评估指标；最后，通过算例分析了信息-物理协同攻击对 IECPS 熵态分布的影响，为统一量化 IECPS 受到攻击后能量的不可用程度提供了手段。

1　IECPS 能量流-信息流混合计算模型

针对由电、气、热 3 种能源形式耦合的 IECPS，本文对其物理层和信息层进行了建模，IECPS 整体架构示意如图 1 所示[15]。在物理层面，多能网络负责电、气、热多能流的传输、转换和消费，其运行状态由馈线终端单元(feeder terminal unit，FTU)、远程控制终端(remote terminal unit，RTU)等传输和控制单元的传感器通过有线或无线网络与控制系统进行通信与控制。在信息层面，能量管理系统则根据多能网络的运行状态，实时做出优化决策，并将指令下发至控制单元的执行器，从而更新能源层的运行状态。

1.1　物理层建模

1.1.1　电网能流模型

电网能流模型基于潮流模型得到，表示如下：

$$\begin{cases} P_i = U_i \sum\limits_{j\in i} U_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \\ Q_i = U_i \sum\limits_{j\in i} U_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}) \end{cases} \tag{1}$$

式中：P_i 和 Q_i 分别为节点 i 的有功和无功功率；U_i 和 U_j 分别为节点 i 和 j 的电压；$j\in i$ 表示节点 i 和 j 相连；G_{ij} 和 B_{ij} 分别为节点 i 和 j 间线路的电导和电纳；θ_{ij} 为节点 i 和 j 电压相角差。

此外，定义 $\boldsymbol{A}_{\mathrm{e}}$ 为阶电网拓扑矩阵，表征电网支路拓扑关系。其中，$\boldsymbol{A}_{\mathrm{e},ij}=1$ 表示存在支路 i - j，$\boldsymbol{A}_{\mathrm{e},ij}=0$ 表示不存在支路 i - j。

1.1.2　气网能流模型

天然气管道流量与管道两端压力，管道长度和直径，工作温度，管道粗糙度等因素有关，本文的模型假设管道理想绝热，考虑天然气的双向流动，其管道流量方程为 Weymouth 方程[16]：

$$M_{\mathrm{g,b},i} = \mathrm{sgn}(p_i, p_j) k_{ij} \sqrt{|\, p_i^2 - p_j^2 \,|} \tag{2}$$

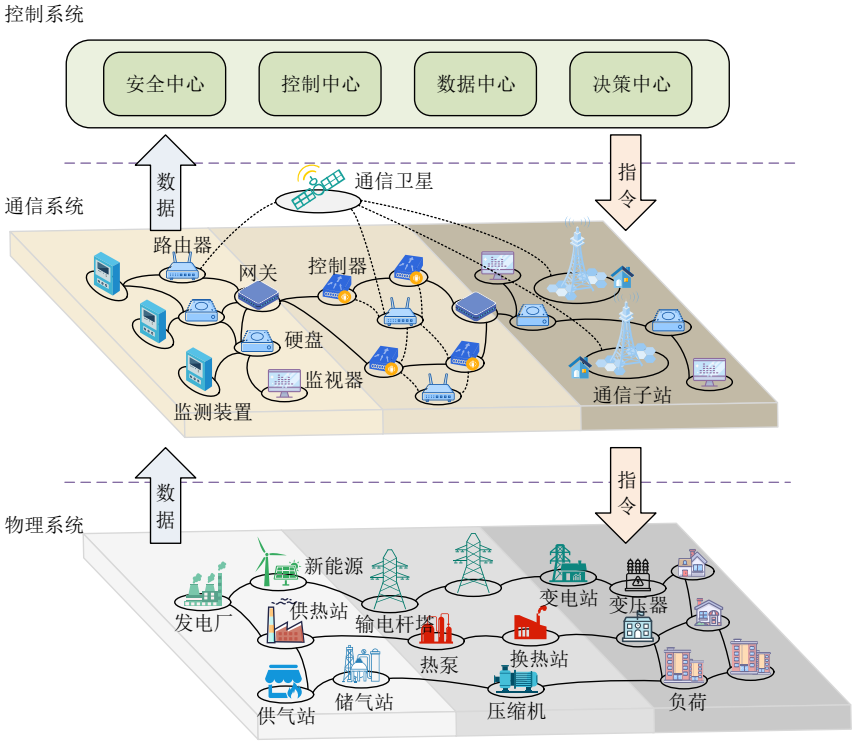


图 1 IECPS 架构示意图

Fig. 1 Schematic diagram of IECPS architecture

$$\mathrm{sgn}=\begin{cases}1, & p_i>p_j\\ -1, & p_i<p_j\end{cases} \tag{3}$$

式中：$M_{\mathrm{g,b}}$ 为天然气支路 i 的流量；k_{ij} 为与管道自身温度、长度、半径、气体密度等因素相关的常数；p_i、p_j 分别为支路 b 两端节点 i、j 的气压。

节点流量平衡方程为

$$\boldsymbol{M}_{\mathrm{g,in}}=\boldsymbol{A}_{\mathrm{g}}\boldsymbol{M}_{\mathrm{g,b}} \tag{4}$$

式中：$\boldsymbol{M}_{\mathrm{g,in}}$ 为节点的注入流量列向量；$\boldsymbol{A}_{\mathrm{g}}$ 为气网关联矩阵；$\boldsymbol{M}_{\mathrm{g,b}}$ 为管道流量矩阵。

环路压力平衡方程为

$$\boldsymbol{B}_{\mathrm{g}}\Delta\boldsymbol{p}_{\mathrm{g}}=0 \tag{5}$$

式中：$\boldsymbol{B}_{\mathrm{g}}$ 为天然气回路的关联矩阵；$\Delta\boldsymbol{p}_{\mathrm{g}}$ 为各支路压力降列向量。

1.1.3 热网能流模型

热网中的水力模型的供水和回水网络具有类似拓扑结构，系统的主干管网为环状，其余为辐射状拓扑，其质量流量方程如下：

$$\boldsymbol{A}_{\mathrm{h}}\boldsymbol{M}_{\mathrm{h,b}}=\boldsymbol{M}_{\mathrm{h,q}} \tag{6}$$

式中：$\boldsymbol{A}_{\mathrm{h}}$ 为区域热力网络的节点-管道关联矩阵；$\boldsymbol{M}_{\mathrm{h,b}}$ 为管道中水的质量流量向量；$\boldsymbol{M}_{\mathrm{h,q}}$ 为注入节点的水的质量流量向量。

水力网络各闭合回路中的水压头损失矢量和为零：

$$\boldsymbol{B}_{\mathrm{h}}\boldsymbol{Z}_{\mathrm{h}}\boldsymbol{M}_{\mathrm{h,b}}\,|\,\boldsymbol{M}_{\mathrm{h,b}}\,|=\boldsymbol{0} \tag{7}$$

式中：$\boldsymbol{B}_{\mathrm{h}}$ 为热力网络回路关联矩阵；$\boldsymbol{Z}_{\mathrm{h}}$ 表示管道的阻抗系数矩阵。

热力模型用于描述热力系统中水温的变化：

$$P_{\mathrm{h,in}}=C_{\mathrm{p}}M_{\mathrm{h},q}(T_{\mathrm{s}}-T_{\mathrm{r}}) \tag{8}$$

式中：$P_{\mathrm{h,in}}$ 为节点注入功率；C_{p} 为水的比热容；T_{s}、T_{r} 分别为节点供水、回水温度。

考虑到管线的热量损失，输送过程中水温的下降可表示为

$$T_{\mathrm{end}}=(T_{\mathrm{enter}}-T_{\mathrm{a}})\mathrm{e}^{\frac{\lambda L}{C_{\mathrm{p}}\dot{m}}}+T_{\mathrm{a}} \tag{9}$$

式中：T_{enter} 为水流入管道时的温度；T_{end} 为水流出管道时的温度；λ 表示管道热传输系数；L 表示管道长度；T_{a} 表示外界环境温度。

多条管道交汇点水流将会混合，对应的混合温度可通过下式计算：

$$(\sum M_{\mathrm{h,b,out}})T_{\mathrm{out}}=\sum(M_{\mathrm{h,b,in}}T_{\mathrm{in}}) \tag{10}$$

式中：$M_{\mathrm{h,b,out}}$ 为管道出口质量流量；T_{out} 为管道出口温度；$M_{\mathrm{h,b,in}}$ 为管道入口的质量流量；T_{in} 为管道入口温度。

1.2 信息层建模

1.2.1 通信通道模型

定义 $\boldsymbol{T}_{k,\mathrm{up}},k\in(\mathrm{e,g,h})$ 为负责将各能源网络和能源站运行数据由能源层传感器上传至传输层通信汇聚子站的上行通信信道矩阵，$\boldsymbol{T}_{k,\mathrm{down}},k\in(\mathrm{e,g,h})$ 为负责将信息层控制指令由传输层通信子站下传

至能源层执行器的下行通信信道矩阵，其中 e、g、h 分别表示电网、气网、热网。上下行通信信道的矩阵 $\boldsymbol{T}_{k,\mathrm{up}}$、$\boldsymbol{T}_{k,\mathrm{down}}$ 表达式分别为

$$\boldsymbol{T}_{k,\mathrm{up}}=\begin{bmatrix} T_{k,\mathrm{up},11} & T_{k,\mathrm{up},12} & \cdots & T_{k,\mathrm{up},1N_k} \\ T_{k,\mathrm{up},21} & T_{k,\mathrm{up},22} & \cdots & T_{k,\mathrm{up},2N_k} \\ \vdots & \vdots & \ddots & \vdots \\ T_{k,\mathrm{up},N_k1} & T_{k,\mathrm{up},N_k2} & \cdots & T_{k,\mathrm{up},N_kN_k} \end{bmatrix} \tag{11}$$

$$\boldsymbol{T}_{k,\mathrm{down}}=\begin{bmatrix} T_{k,\mathrm{down},11} & T_{k,\mathrm{down},12} & \cdots & T_{k,\mathrm{down},1N_k} \\ T_{k,\mathrm{down},21} & T_{k,\mathrm{down},22} & \cdots & T_{k,\mathrm{down},2N_k} \\ \vdots & \vdots & \ddots & \vdots \\ T_{k,\mathrm{down},N_k1} & T_{k,\mathrm{down},N_k2} & \cdots & T_{k,\mathrm{down},N_kN_k} \end{bmatrix} \tag{12}$$

式中：两个通信信道矩阵中的元素 $T_{k,\mathrm{up},ij}$ 与 $T_{k,\mathrm{down},ij}$ 均由 1 和 0 组成，元素为 1 表示对应能源层各节点或支路的控制单元与通信子站之间存在上传或下传通道，元素为 0 表示不存在该通道。

1.2.2　信息-能量流耦合计算模型

能源网络的能流分布可通过潮流计算快速求解，而信息流与能量流间的相互转换可描述为线性映射。其转换关系如下：

1）能量流→信息流。

该过程的目的是实现物理状态到虚拟信号的转换，即将物理状态量映射为信息输入，该过程描述为

$$\boldsymbol{I}_k^{\mathrm{up}}=\boldsymbol{C}_k^{\mathrm{up}}\odot\boldsymbol{P}_k\odot\boldsymbol{T}_{k,\mathrm{up}} \tag{13}$$

式中：$\boldsymbol{I}_k^{\mathrm{up}}$ 为能量流转换为上传信息流的信息矩阵；$\boldsymbol{P}_k$ 为对应能源网络的能流矩阵；$\boldsymbol{C}_k^{\mathrm{up}}$ 为能量流转换为信息流的映射矩阵，$k\in(\mathrm{e},\mathrm{g},\mathrm{h})$；$\odot$ 符号表示矩阵中对应元素相乘。

2）信息流→能量流。

该环节对应实际系统的控制环节，即将信息网络中的决策信息映射为实际的控制量，可描述为

$$\boldsymbol{I}_k^{\mathrm{down}}=\boldsymbol{C}_k^{\mathrm{down}}\odot\boldsymbol{I}_k\odot\boldsymbol{T}_{k,\mathrm{down}} \tag{14}$$

式中：$\boldsymbol{I}_k^{\mathrm{down}}$ 为信息流转换为实际下达控制量的信息矩阵；$\boldsymbol{C}_k^{\mathrm{down}}$ 为信息流转换为能量流的映射矩阵；$\boldsymbol{I}_k$ 为各能源网络控制中心的决策信息；$k\in(\mathrm{e},\mathrm{g},\mathrm{h})$。

1.2.3　控制中心模型

1）目标函数。

针对 IECPS 受到物理、信息攻击时可能出现的支路越限现象，本文以各能源网络负荷削减量最小为优化决策目标[17-19]，建立目标函数如下：

$$\min f=\sum_{i=1}^{N_\mathrm{e}}(\Delta P_{\mathrm{e},i})^2+\sum_{j=1}^{N_\mathrm{h}}(\Delta P_{\mathrm{h},j})^2+\sum_{k=1}^{N_\mathrm{g}}(\Delta P_{\mathrm{g},k})^2 \tag{15}$$

式中：N_e、N_h、N_g 分别为电网、热网、气网的节点数量；$\Delta P_{\mathrm{e},i}$、$\Delta P_{\mathrm{h},j}$、$\Delta P_{\mathrm{g},k}$ 分别为电网、热网、气网 i、j、k 节点负荷削减量；$P_{\mathrm{e},i}$、$P_{\mathrm{h},j}$、$P_{\mathrm{g},k}$ 分别代表电网、热网、气网负荷节点 i、j、k 的负荷功率。

其中，气负荷节点 k 的负荷功率计算公式如下：

$$P_{\mathrm{g},k}=GM_{\mathrm{g,in},k} \tag{16}$$

式中：G 为天然气的热值；$M_{\mathrm{g,in},k}$ 为气负荷节点 k 的注入流量。

2）约束条件。

电网能流约束表示如式(17)所示，分别为电网有功平衡约束、发电机出力约束、线路容量约束、电负荷削减约束。

$$\begin{cases} \sum_{i=1}^{N_\mathrm{e}}P_{\mathrm{e},i}+\sum_{j=1}^{B_\mathrm{e}}P_{\mathrm{loss},j}-\sum_{k=1}^{N_k}P_{\mathrm{out},k}=0 \\ P_{\mathrm{out}i\min}\le P_{\mathrm{out},i}\le P_{\mathrm{out}i\max} \\ -P_{\mathrm{eb}i\max}\le P_{\mathrm{e,bran},i}\le P_{\mathrm{eb}i\max} \\ 0\le\Delta P_{\mathrm{e},i}\le P_{\mathrm{e},i} \end{cases} \tag{17}$$

式中：B_e 为电网支路的数量；N_k 为电网中发电节点的数量，包括发电机和分布式能源；$P_{\mathrm{e},i}$ 为电网第 i 个节点的负荷功率；$P_{\mathrm{loss},j}$ 为电网第 j 条线路损耗；$P_{\mathrm{out},k}$ 为第 k 台发电机、能源站节点或上级电网注入功率；$P_{\mathrm{out}i\max}$、$P_{\mathrm{out}i\min}$ 分别为发电机、能源站设备出力功率上下限；$P_{\mathrm{eb}i\max}$ 为电网线路容量上限。

气网能量约束表示如式(18)所示，分别为流量平衡约束、气源出力约束、管道流量约束、节点压力约束、负荷节点气流量削减约束。

$$\begin{cases} \sum_{i=1}^{N_\mathrm{g,in}}m_{\mathrm{g,in},i}-\sum_{j=1}^{N_\mathrm{g}}m_{\mathrm{g},j}=0 \\ m_{\mathrm{g},i,\min}\le m_{\mathrm{g},i}\le m_{\mathrm{g},i,\max} \\ m_{\mathrm{g,b},i,\min}\le m_{\mathrm{g,b},i}\le m_{\mathrm{g,b},i,\max} \\ 0\le\Delta m_{\mathrm{g},i}\le m_{\mathrm{g},i} \end{cases} \tag{18}$$

式中：$N_\mathrm{g,in}$ 为气源节点的数量；$m_{\mathrm{g,in},i}$ 为第 i 个气源节点的注入流量；$m_{\mathrm{g},j}$ 为第 j 个负荷流量；$m_{\mathrm{g},i,\max}$、$m_{\mathrm{g},i,\min}$ 为气源出力流量上下限；$m_{\mathrm{g,b},i,\max}$、$m_{\mathrm{g,b},i,\min}$ 为管道运输天然气流量上下限。

热网能量约束表示如式(19)所示，分别为流量平衡约束、热源出力约束、管道流量约束、负荷节点水流量削减约束。

$$\begin{cases} \sum_{i=1}^{N_\mathrm{h}}m_{\mathrm{h,L},i}-\sum_{k=1}^{N_k}m_{\mathrm{out},k}=0 \\ m_{\mathrm{out},i,\min}\le m_{\mathrm{out},i}\le m_{\mathrm{out},i,\max} \\ m_{\mathrm{h,b},i,\min}\le m_{\mathrm{h,b},i}\le m_{\mathrm{h,b},i,\max} \\ 0\le\Delta m_{\mathrm{h},i}\le m_{\mathrm{h},i} \end{cases} \tag{19}$$

式中：$m_{\mathrm{h,L},i}$ 为第 i 个负荷节点注入流量；$m_{\mathrm{out},k}$ 为

第 k 个热源节点的注入流量；$m_{\mathrm{out},i,\max}$、$m_{\mathrm{out},i,\min}$ 分别为热源出力流量上下限；$m_{\mathrm{h,b},i,\max}$、$m_{\mathrm{h,b},i,\min}$ 分别为管道运输流量上下限。

2 网络攻击下的 IECPS 熵态模型

当信息攻击成功作用于能量管理系统时，会影响系统的运行状态及其对能量的利用效率，进而出现“能量退化”现象。为量化网络攻击对系统“能量退化”的影响，首先需要建立网络攻击模型，以明确其对系统能量数据的篡改程度。在此基础上，建立信息攻击熵增模型，将信息攻击视作一种特殊的“功”，量化其作用下系统的“能量退化”程度。最后，提出基于潮流熵的网络攻击对系统的物理影响指标，量化能源网络中节点和支路受网络攻击的扰动程度。

2.1 网络攻击模型

针对 IECPS 的信息攻击是指以破坏或降低 IECPS 供能能力为目的，蓄意对通信系统和控制系统的各个环节进行追踪，并利用通信网络存在的漏洞和安全隐患对系统本身或资源进行攻击。按照破坏网络安全三要素，信息攻击可分为信息完整性攻击、可用性攻击和保密性攻击[15]。

通过归纳不同类型信息攻击的目标，控制中心与物理系统的交互过程可以视为一种“物理-信息-物理”的过程。其中，测量和控制设备及其建立的通信通道在信息网络和物理系统中起连接作用。本文主要关注信息网络被攻击成功后对 IECPS 运行状态的影响，因此在信息攻击建模中不考虑具体攻击策略，而只对成功绕过信息网络防御后，信息攻击对通信和控制系统能量数据的篡改过程进行建模。综上所述，IECPS 上下行通信及信息攻击示意如图 2 所示。

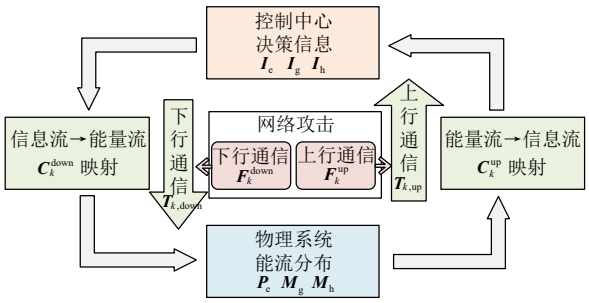


图 2 IECPS 通信及信息攻击示意图

Fig. 2 IECPS communication and cyber attack schematic

1）在上行通信中，篡改传感器设备的测量数据，使控制中心接收的数据信息与实际状态量不一致，从而间接影响控制决策。

2）在下行通信中，发送虚假的数据决策指令，篡改 RTU 执行器接收到的指令，直接改变系统的正常控制措施。

故需要针对上下行通信通道分别进行建模，定义矩阵 $\boldsymbol{F}_k^{\mathrm{up}}$、$\boldsymbol{F}_k^{\mathrm{down}}$ 分别为上下行通信通道的信息攻击矩阵。

$$\boldsymbol{F}_k^{\mathrm{up}}=\begin{bmatrix} f_{\mathrm{up}11} & f_{\mathrm{up}12} & \cdots & f_{\mathrm{up}1N_k} \\ f_{\mathrm{up}21} & f_{\mathrm{up}22} & \cdots & f_{\mathrm{up}2N_k} \\ \vdots & \vdots & \cdots & \vdots \\ f_{\mathrm{up}N_k1} & f_{\mathrm{up}N_k2} & \cdots & f_{\mathrm{up}N_kN_k} \end{bmatrix} \tag{20}$$

$$\boldsymbol{F}_k^{\mathrm{down}}=\begin{bmatrix} f_{\mathrm{down}11} & f_{\mathrm{down}12} & \cdots & f_{\mathrm{down}1N_k} \\ f_{\mathrm{down}21} & f_{\mathrm{down}22} & \cdots & f_{\mathrm{down}2N_k} \\ \vdots & \vdots & \cdots & \vdots \\ f_{\mathrm{down}N_k1} & f_{\mathrm{down}N_k2} & \cdots & f_{\mathrm{down}N_kN_k} \end{bmatrix} \tag{21}$$

式中：矩阵元素 $f_{\mathrm{up}ij}$、$f_{\mathrm{down}ij}$ 分别为系统上行和下行潮流信息的篡改程度。

当能源网络的某条电力线路或供气、供热管道受到物理性攻击而断开或能流承载能力下降时，可直接修改对应网络的拓扑矩阵 $\boldsymbol{A}_k$ 与支路潮流约束条件，重新求解系统潮流，因此物理攻击后的系统能量状态可根据 1.1 节物理层模型以及 1.2.3 节控制中心决策模型重新求解得到，此处不再赘述。

2.2 信息攻击熵增模型

2.2.1 基于攻击图的信息攻击概率计算

攻击图可以表征攻击者为完成对攻击目标的成功攻击所实施的攻击路径，通过对攻击路径的分析进而计算信息攻击成功的概率[20-21]。具体计算方式见附录 A 所示，此处不再赘述。

2.2.2 信息攻击的熵增计算模型

当有效信息输入能量管理系统，可以使能量被更有效地利用，从而降低系统的热力学熵增。故在能源系统中，可以将信息视为一种特殊的“功”[22]，并通过信息熵来量化系统状态变化导致的能量不可用性。广义信息功指系统基于信息，通过控制等技术克服由于不确定性导致的能量不可被利用，进而产生有用功，而非信息直接做功，广义信息功的计算方法[12,23]为

$$W_{\mathrm{i}}=p_i i \tag{22}$$

式中：信息势 p_i 为单位微观状态改变所能引起的能量变化；i 为信息流。

对考虑不确定性的能量变化进行归一化处理，进而信息流可以表示为

$$i=H=-\sum_{n=1}^{s}P_n(x)\ln P_n(x) \tag{23}$$

式中：H 为信息熵，单位 nat；$P_n(x)$ 为归一化后的

能量变化处于第 n 个微观状态的概率；s 为能量变化的微观状态个数。

对于不确定性能量变化，信息势可以表示为

$$p_{\mathrm{i}}=\frac{P_{\max}-P_{\min}}{s} \tag{24}$$

式中：$P_{\max}$ 和 $P_{\min}$ 分别为能量变化范围的上下限，kW。

于是，当原本可以被利用的能量由于信息的作用而没有被有效利用时，该部分信息“功”用熵增表示为

$$\Delta S_{\mathrm{i}}=\frac{W_{\mathrm{i}}}{T_a}=\frac{p_{\mathrm{i}} f_{\mathrm{i}}}{T_a} \tag{25}$$

式中：为信息熵等效热力学熵增。

信息攻击的作用效果是通过改变信息系统接收的潮流信息或发出的控制信号，进而改变物理系统的潮流分布。因此，计算攻击下的热力学熵的关键在于计算攻击作用于系统的能量变化。基于此，以下针对信息的上行和下行通信过程，分别提出能量变化的计算公式：

1）对于上行通信，信息攻击作用于遥测设备读取的系统潮流数据时，此微观状态的能量变化描述为

$$\Delta \boldsymbol{P}_k^{\mathrm{up}}=\boldsymbol{P}_k-\boldsymbol{F}_k^{\mathrm{up}}\odot\boldsymbol{I}_k \tag{26}$$

式中：$\Delta \boldsymbol{P}_k^{\mathrm{up}}$ 为信息攻击作用于上行通信过程对某能源网络造成的能量变化矩阵。

2）对于下行通信，信息攻击作用于控制中心下达的决策信息，具体表现为 1.2.2 小节下行通道的信息流→能量流通信数据被篡改，此状态的能量变化描述为

$$\Delta \boldsymbol{P}_k^{\mathrm{down}}=\boldsymbol{P}_k-\boldsymbol{F}_k^{\mathrm{down}}\odot\boldsymbol{I}_k^{\mathrm{down}} \tag{27}$$

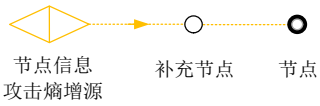
式中：$\Delta \boldsymbol{P}_k^{\mathrm{down}}$ 为信息攻击作用于下行通信过程对某能源网络造成的能量变化矩阵。

当没有受到信息攻击时，认为系统的宏观变化为零，即没有能量变化。综上，定义信息攻击下系统的信息等效热力学熵为信息攻击熵增(cyber attack entropy increase，CAEI)，以某个节点或管线为例，信息攻击产生的信息攻击熵增可表示为

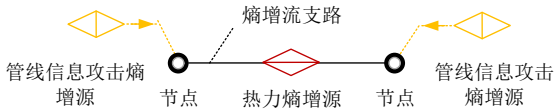
$$\Delta S_{k,ij}^{\mathrm{up/down}}=[-\sum_{n=1}^{2}P_{ijn}\ln P_{ijn}]\frac{|\Delta P_{k,ij}^{\mathrm{up/down}}|}{2T_{\mathrm{a}}} \tag{28}$$

式中：$\Delta S_{k,ij}^{\mathrm{up/down}}$ 为电网的某个节点或支路潮流状态的上行或下行通信受到信息攻击的熵增，单位 kW/K；$\Delta P_{k,ij}^{\mathrm{up/down}}$ 为能源网络的某个节点或支路受到信息攻击后的能量变化，单位 kW；P_{ijn} 为节点或管线是否成功受到信息攻击的概率，n=1 代表成功受到信息攻击，n=2 代表未受到信息攻击，$k\in(\mathrm{e},\mathrm{g},\mathrm{h})$；$T_{\mathrm{a}}$ 为环境温度。

建立信息攻击熵增源如图 3 所示。具体而言，图 3(a)表示物理系统中某节点所在的通信网络受到信息攻击时的信息熵增示意，信息攻击成功后，根据攻击路径的差异性，该节点的能量变化如式(26)或式(27)所示。进一步地，结合式(22)—(25)对信息等效热力学熵的计算推论，可得到如式(28)所示的信息攻击熵增模型。图 3(b)表示物理系统中某管线所在的通信网络受到信息攻击时的熵增示意，信息攻击成功作用于管线的信息攻击熵增计算与节点信息攻击熵增类似，均只关注信息攻击造成元件的能流变化量和攻击成功的概率。需要注意的是，考虑到受攻击后管线出现开断的情况，会直接或间接影响管线两端的物理节点，因此，其信息攻击熵增应平均分配到管线两端的物理节点，并在网络中流动，遵循节点熵增流分配定律[13]。



(a) 节点信息攻击熵增示意图



(b) 管线信息攻击熵增示意图

图 3　信息攻击熵增源示意图

Fig. 3　Schematic diagram of cyber attack entropy increase source

2.3　基于潮流熵的网络攻击下物理影响评估指标

2.2 节中提出了由于信息攻击具有的不确定性给系统带来的熵增计算方法，用于量化信息攻击造成系统能量不可被利用的程度，本节则聚焦于当系统受到网络攻击后的运行状态，提出网络攻击对物理系统扰动程度的量化指标。

IES 作为一个能量平衡系统，其内部的稳定平衡可以通过系统内部能量分布的“熵变”过程来描述，故把潮流熵[24]引入 IES 中，综合分析网络攻击带来的影响是可行的。因此，本节基于潮流分布熵和潮流转移熵分别提出针对能源网络中节点、支路受网络攻击对系统扰动程度的量化评估指标。

2.3.1　基于潮流分布熵的系统节点影响评估指标

传统潮流分布熵反映了节点受到扰动后的能量变化对系统支路造成的冲击效应，为了统一度量，本节定义基于潮流分布熵的系统节点影响评估指标——潮流分布熵等效热力学熵增。

系统受到网络攻击后节点 m 能量变化引起支

路 n 产生的能量变化为

$$\Delta P_{nm} = P_{n0} - P_{nm} \tag{29}$$

式中：P_{n0} 为基态下支路 n 的潮流，单位 kW；P_{nm} 为节点 m 产生能量变化后，支路 n 的潮流，单位 kW。

节点 m 能量变化而引起系统支路产生的能量变化 $\Delta P_{sm}^{\text{total}}$ 为

$$\Delta P_{sm}^{\text{total}} = \sum_{m=1}^{S}(P_{m0} - P_{mn}) \tag{30}$$

式中：S 为系统的总支路数；P_{m0} 为基态下节点 m 的潮流。

支路 n 承担由于节点 m 能量变化对系统产生的能量变化比例 γ_{nm} 为

$$\gamma_{nm} = \frac{\Delta P_{nm}}{\Delta P_{sm}^{\text{total}}} \tag{31}$$

节点 m 的潮流分布熵等效热力学熵增为

$$\Delta S_{\text{pfd},m} = [-\sum_{i=1}^{S}\gamma_{im}\ln\gamma_{im}]\frac{|\Delta P_m|}{ST_a} \tag{32}$$

式中：ΔP_m 为节点 m 的能量变化量；$\Delta S_{\text{pfd},m}$ 为节点 m 受网络攻击对系统扰动程度指标，$\Delta S_{\text{pfd},m}$ 越大，表示该节点受扰动对系统的潮流冲击越大，当系统中节点受网络攻击扰动而出现能量变化时，需要计算该熵增。

2.3.2 基于潮流转移熵的系统支路影响评估指标

传统潮流分布熵反映支路退出运行后对系统的影响，为了统一度量，本节定义基于潮流转移熵的系统支路影响评估指标——潮流转移熵等效热力学熵增。

当系统中支路 i 断开时，支路 k 分担支路 i 转移的能量增量为

$$\Delta P_{ki} = P_{ki} - P_{k0} \tag{33}$$

式中：P_{ki} 为支路 i 断开后支路 k 的潮流，kW；P_{k0} 为系统基态下支路 k 的潮流，kW。

支路 i 对支路 k 的潮流转移冲击率为

$$\eta_{ki} = \frac{\Delta P_{ki}}{\sum_{n=1}^{S}\Delta P_{ni}} \tag{34}$$

支路 i 的潮流转移熵等效热力学熵增为

$$\Delta S_{\text{pft},i} = [-\sum_{k=1}^{S}\gamma_{ki}\ln\gamma_{ki}]\cdot\frac{|P_{i0}|}{S\cdot T_a} \tag{35}$$

式中：$\Delta S_{\text{pft},i}$ 为支路 i 受网络攻击对系统扰动程度的指标，$\Delta S_{\text{pft},i}$ 越大，表示该支路受扰动对系统 l_{e2} 的潮流冲击越大，当系统因受网络攻击扰动而开断时，需要计算该熵增。

2.4 求解流程

基于 1.1、1.2 节所提出的 IECPS 能量流-信息流混合计算模型，计算流程如附录 A 图 A2 所示，首先求解出物理/信息攻击后的 IECPS 物理系统潮流，若受攻击后出现支路越限的情况，则控制系统进行负荷削减优化，下达指令后潮流重新分布，求解计算 IES烟流后，进而求解系统熵态分布。系统受到网络攻击前后的运行状态以及各状态下的熵增和物理指标计算示意如图 4 所示，在网络攻击成功前，系统的源荷不确定性熵增和传统热力学熵增即存在。当网络攻击成功后，系统便进入过渡状态，能量管理系统开始工作，发出切负荷指令，系统进入新的稳定运行状态后，重新计算的源荷不确定性熵增和传统热力学熵增，新增计算信息攻击熵增和网络攻击后的物理影响熵增。

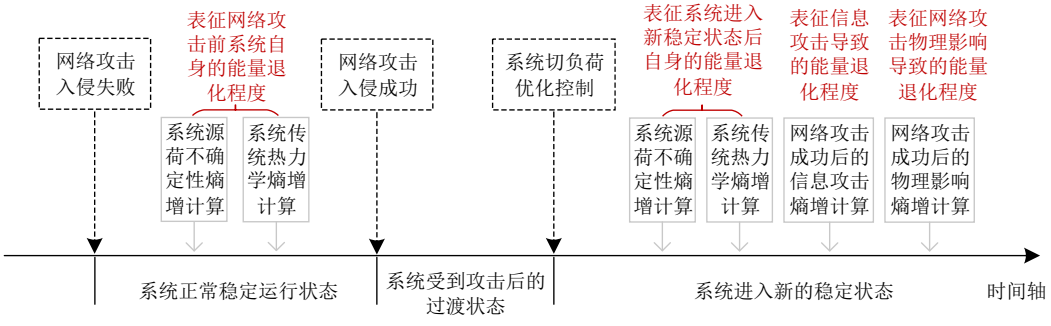


图 4 网络攻击前后系统运行状态及指标计算示意图

Fig. 4 Schematic diagram of system running state and index calculation before and after network attack

3 算例分析

3.1 算例介绍

本文构建了一个基于典型区域的 IECPS 算例测试系统[25-27]，如附录 A 图 A3 所示，系统介绍见附录 A。

为验证前述网络攻击熵态模型的有效性，本文以攻击方通过破坏能源网络的线路或管道，使其产生故障而断开或出现承载能力下降的问题，作为物理攻击手段；以攻击方通过网络攻击篡改控制中心接收的物理系统潮流信息或下达的控制指令，作为信息攻击方式。基于以上物理、信息攻击方式，设

置如下场景：

场景一：不受攻击。该场景下 IECPS 能源网络和信息网络均正常运行，以此作为对照场景。

场景二：系统仅受物理攻击。强攻击场景下，线路或管道受到物理攻击而断开，本文选取电网线路 l_{e2}、气网管道 l_{g5}、热网管道 l_{s4} 作为受到攻击的目标；弱攻击场景下，物理攻击导致线路或管道的承载能力下降，从而出现支路过载现象，本文选取电网线路 l_{e5}、气网管道 l_{g4}、热网管道 l_{s2} 作为攻击目标。

场景三：仅系统的上行通信环节受网络攻击。攻击方对信息采集装置进行 FDI 攻击，将其采集的正常潮流信息篡改为越限状态，导致控制中心收到异常信息而进行负荷削减优化决策。本文选取电网线路 l_{e2}、气网管道 l_{g5}、热网管道 l_{s4} 所对应上行通信矩阵中的能量流→信息流通信环节作为攻击目标。

场景四：仅系统的下行通信环节受网络攻击。攻击方对控制中心进行 FDI 攻击，将原本正常的运行控制指令篡改为切负荷指令。本文选取电力节点 E_2、天然气节点 G_3、热力节点 H_3 的指令下达环节作为攻击目标，其中，电力节点 E_2 切负荷 30kW、天然气节点 G_3 切负荷 40m^3/h、热力节点 H_3 切负荷 0.2kg/s。

场景五：系统受到信息-物理协同攻击。设置为对电力线路 l_{e5} 进行物理攻击，导致线路承载能力下降，同时对能量管理系统的数据进行 DoS 攻击，导致其拒绝对支路越限情况做出负荷优化指令。

3.2　结果分析

根据 2.4 节求解流程，分别求解 3.1 节所设置的 5 个场景的系统能流以及熵态分布。各场景信息攻击成功的概率计算结果如附录 C 表 C4 所示，5 种场景设置情况及其对应的部分重要结果如附录 C 表 C5 所示，算例计算的具体结果分析详见 3.2.1-3.2.5 节各场景结果分析。

3.2.1　场景一

当系统没有受到攻击时，IECPS 能源网络和信息网络正常运行，无设备故障和网络攻击的干扰，能量-信息流混合计算便等同于单独的能流计算。系统负荷计算结果见附录 B 图 B1，系统潮流结果见附录 C 表 C6。

根据算例系统求解熵态模型，根据上述参数与模型求解方法，绘制系统某一时间断面下的熵态网络如附录 B 图 B2 所示，在该场景下，由于系统没有受到物理或网络攻击，故注入节点的信息等效热力学熵增仅由源荷自身不确定性产生。

3.2.2　场景二

在场景二(1)中，电网线路 l_{e2} 受到物理攻击永久性断开后潮流重新分布，其相邻支路 l_{e3}、l_{e5}、l_{e6} 由于支路功率越限而暂时断开，此时远程采集和控制终端将越限信息和支路状态信息(通过信息传输层的矩阵)上传给控制中心，控制中心以最优负荷削减量为目标做出优化决策指令。执行指令后越限现象消失，控制中心发出合闸指令，执行指令后的系统节点注入/输出能流如附录 B 图 B3 所示，电网共失负荷 170.22kW，气网共失负荷 36.07m^3/h，热网共失负荷 0.63kg/s，系统潮流如附录 C 表 C7 所示。由于系统同时出现负荷损失和支路开断的情况，故系统的潮流分布熵与潮流转移熵等效热力学熵增同时存在，分别为 0.1266 kW/K 和 0.2874 kW/K。

根据算例系统求解熵态模型，绘制系统的熵态网络如附录 B 图 B4 所示。

在场景二(2)中，电网线路 l_{e5}、气网管道 l_{g4}、热网管道 l_{s2} 受物理破坏而承载能力下降，此时远程采集和控制终端将支路潮流越限信息和支路状态信息上传至能量管理系统，系统发出支路 l_{e5}、l_{g4}、l_{s2} 开断指令，同时以最优负荷削减量为优化目标做出决策指令。指令执行后，控制系统接收的越限信息消除，发出合闸指令，执行指令后的系统节点注入/输出能流如附录 B 图 B5 所示，配电网共失负荷 69.66kW，配气网共失负荷 38.73m^3/h，供热网共失负荷 0.14kg/s，系统潮流如附录 C 表 C8 所示。系统仅出现负荷损失的情况，因此仅存在潮流分布熵等效热力学熵增为 0.1064 kW/K，相较于本场景强攻击下的“潮流熵信息等效热力学熵增”以及能量损失情况，不难看出弱攻击对系统稳定性造成的不良影响较小。

根据算例系统求解熵态模型，绘制系统的熵态网络如附录 B 图 B6 所示。

3.2.3　场景三

对于仅上行通信 $\boldsymbol{T}_{k,\mathrm{up}}$ 受网络攻击场景。管线 l_{e2}、l_{g5}、l_{s4} 的信息采集装置采集的正常潮流信息被篡改为越限状态，即控制中心收到异常信息而进行负荷削减优化决策。在该情况下，控制中心以最优负荷削减量为目标做出优化决策指令，执行指令后的系统节点注入/输出能流如附录 B 图 B7 所示。配电网共失负荷 88.77kW，气网共失负荷 52.51m^3/h，热网共损失负荷 0.4kg/s，系统潮流如附录 C 表 C9 所示。该场景下，系统潮流分布熵等效热力学熵增为 0.1621 kW/K。

根据算例系统求解熵态模型，根据上述参数与模型求解方法，绘制系统的熵态网络如附录 B 图 B8 所示。

3.2.4 场景四

对于仅下行通信 $\boldsymbol{T}_{k,\mathrm{down}}$ 受网络攻击场景，攻击方对控制中心下达的决策指令进行篡改，将原本正常的运行控制指令篡改为切负荷指令后，系统节点注入/输出能流如附录 B 图 B9 所示，配电网共失负荷 30kW，气网共失负荷 40m^3/h，热网共损失负荷 0.2kg/s，系统潮流如附录 C 表 C10 所示。该场景下，系统的潮流分布熵等效热力学熵增为 0.0924 kW/K，相较于场景三有所下降，而该场景的负荷损失情况弱于场景三，验证了本文所提物理影响评估指标的有效性。

根据算例系统求解熵态模型，根据上述参数与模型求解方法，绘制系统的熵态网络如附录 B 图 B10 所示。

3.2.5 场景五

对电力线路 l_{e5} 进行物理攻击导致线路承载能力下降，同时对能量管理系统的数据进行 DoS 攻击，导致能量管理系统拒绝对支路越限情况做出优化负荷指令。此时，越限问题无法解决，支路重合闸失败，并间接导致支路 l_{e1}、l_{e3}、l_{e6} 潮流越限而跳闸断开，且负荷节点 E_1、E_3 退出运行。系统节点注入/输出能流如附录 B 图 B11 所示，配电网共损失负荷 190kW，由于存在能源站多能耦合环节，间接导致气网损失负荷 34.08m^3/h，热网损失负荷 0.23kg/s，系统潮流如附录 C 表 C11 所示。在信息-物理协同攻击下，由于 IECPS 存在信息-物理耦合与多能耦合环节，原本由物理攻击造成系统供能下降的情况会因信息攻击而进一步恶化，且由于 IES 多能耦合环节的存在，该不良影响会从单一能源系统扩大至其他能源系统。

根据算例系统求解熵态模型，绘制场景一与该场景的熵态网络对比如图 5 所示。由于网络攻击作用于支路 l_{e5} 而产生的信息攻击熵增总量为 0.2430 kW/K，而由于控制系统优化负荷功能失效，最终导致节点 E_3 退出运行，本该由节点 E_3 承担的 0.1215 kW/K 的信息攻击熵增现由节点 E_7 承担。从网络攻击对系统的物理影响来看，该场景下系统的潮流分布熵等效热力学熵增与潮流转移熵等效热力学熵增之和为 0.4816 kW/K，高于其他场景，表明系统的节点、支路受信息-物理协同攻击的影响较大，对系统稳定性造成的不良影响较大。

通过对场景二~场景五的仿真结果对比分析，相较于传统信息物理耦合系统网络攻击以及能量系统的“熵”研究，本文所建立模型以及提出的指标能够统一刻画网络攻击导致能量的退化程度，以及量化网络攻击成功后系统节点和支路能量供应的破坏情况，有助于分别明确二者对系统能量退化的影响程度。

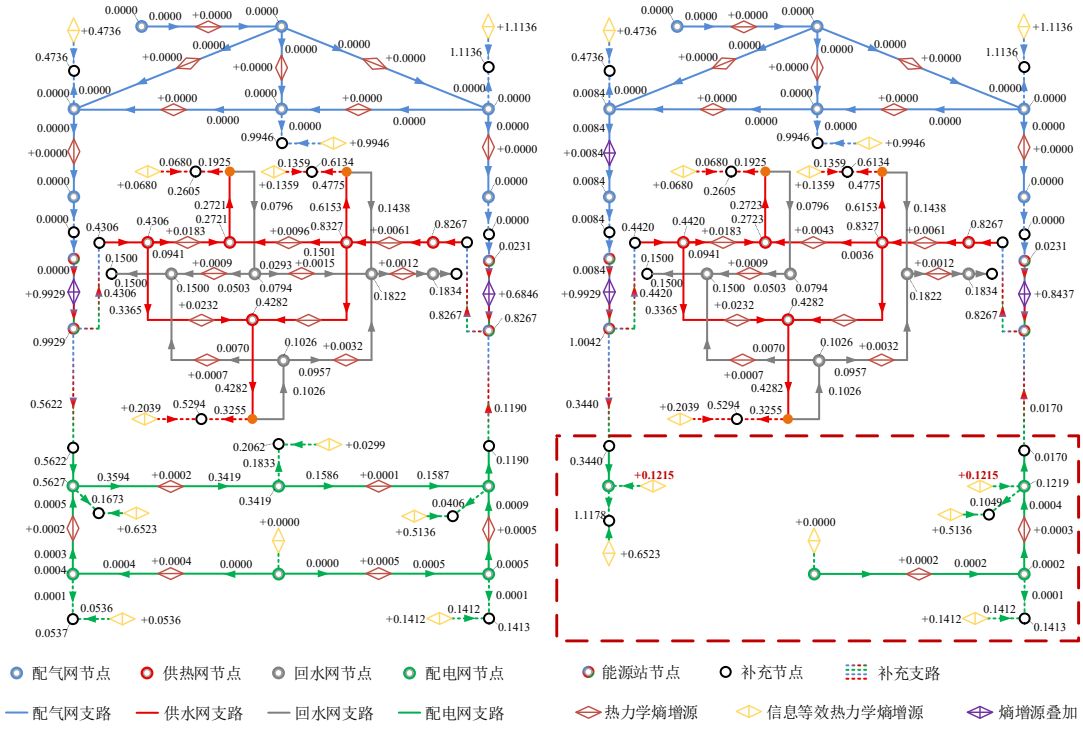


图 5 场景五网络攻击下系统受到攻击前后熵态图对比

Fig. 5 Comparison of entropy state diagram before and after network attack in scenario 5

4　结论

本文基于 IES烟流和熵态机理模型，以及信息物理系统中信息-物理协同攻击手段及特性，提出了综合能源信息物理系统的熵态建模与故障分析方法，主要工作及结论如下：

1）首先提出了 IECPS 的信息流-能量流融合建模方法，通过建立信息-能量流耦合计算模型，为信息流与能量流之间的相互转换提供了一种快速计算方式。该模型明确了 IECPS 在正常运行状态下的能量流动和信息传递过程，同时为分析网络攻击下系统稳定性奠定了理论基础。

2）其次，在考虑网络攻击给能源系统造成实际物理层面影响的基础上，建立了网络攻击的信息等效热力学熵增模型及其物理影响的评估指标，既统一刻画了传统源荷不确定性、网络攻击导致能量的退化程度，又量化描述了攻击发生后系统节点和支路能量供应的破坏情况。

3）通过算例分析，验证了所提模型的有效性。在稳态场景下，系统能流和熵态分布得到了准确计算；在网络攻击场景下，系统能流和熵态的变化被成功捕捉，展示了网络攻击对系统能量可用性的显著影响，为统一量化 IECPS 受到网络攻击后能量的不可用程度以及系统受网络攻击的扰动程度提供了手段。

综上所述，本文提出的网络攻击下综合能源信息物理系统熵态模型为综合能源系统的安全防御提供了新的视角和方法，作者的后续工作将进一步探究不同类型的网络攻击对综合能源信息物理系统(IECPS)能量退化的影响，建立网络动态特性下的信息攻击熵增模型以及系统熵态模型，并深入分析 IECPS 能量耦合环节受到网络攻击对系统的影响。

附录见本刊网络版(http://www.dwjs.com.cn/CN/1000-3673/current.shtml)。

参考文献

[1] 郭庆来，辛蜀骏，孙宏斌，等．电力系统信息物理融合建模与综合安全评估：驱动力与研究构想[J]．中国电机工程学报，2016，36(6)：1481-1489．
GUO Qinglai，XIN Shujun，SUN Hongbin，et al．Power system Cyber-physical modelling and security assessment：motivation and ideas [J]．Proceedings of the CSEE，2016，36(6)：1481-1489(in Chinese)．

[2] 郑琨琪，王治华，范帅，等．电网信息物理系统的数据驱动架构设计及应用[J]．电网技术，2018，42(10)：3116-3127．
JIA Kunqi，WANG Zhihua，FAN Shuai，et al．Data-driven architecture design and application of power grid cyber physical system[J]．Power System Technology，2018，42(10)：3116-3127(in Chinese)．

[3] GEORG H，MÜLLER S C，REHTANZ C，et al．Analyzing cyber-physical energy systems：The INSPIRE cosimulation of power and ICT systems using HLA[J]．IEEE Transactions on Industrial Informatics，2014，10(4)：2364-2373．

[4] 加鹤萍，丁一，宋永华，等．信息物理深度融合背景下综合能源系统可靠性分析评述[J]．电网技术，2019，43(1)：1-11．
JIA Heping，DING Yi，SONG Yonghua，et al．Review of reliability analysis for integrated energy systems with integration of cyber physical systems[J]．Power System Technology，2019，43(1)：1-11(in Chinese)．

[5] 叶学顺，李昭，刘科研，等．信息物理并发故障下的配电网供电恢复方法[J]．电力信息与通信技术，2024，22(9)：18-25．
YE Xueshun，LI Zhao，LIU Keyan，et al．Distribution network power restoration under cyber-physical concurrent faults[J]．Electric Power Information and Communication Technology，2024，22(9)：18-25(in Chinese)．

[6] 杨挺，李浩，赵宇明，等．电力信息物理系统故障通信恢复策略[J]．电网技术，2025，49(1)：381-389．
YANG Ting，LI Hao，ZHAO Yuming，et al．Fault communication recovery strategy of power cyber-physical system[J]．Power System Technology，2025，49(1)：381-389(in Chinese)．

[7] 赵宇龙，刘春明，付晴玉，等．考虑多重耦合关系的电力信息物理系统协同攻击研究[J/OL]．电网技术，2025：1-13[2025-5-28]．https://doi.org/10.13335/j.1000-3673.pst.2024.0651．
ZHAO Yulong，LIU Chunming，FU Qingyu，et al．Research on collaborative attacks on cyber-physical power system considering multiple coupling relationships[J/OL]．Power System Technology，2025：1-13[2025-5-28]．https://doi.org/10.13335/j.1000-3673.pst.2024.0651 (in Chinese)．

[8] BO Xiaoyong，QU Zhaoyang，WANG Lei，et al．Active defense research against false data injection attacks of power CPS based on data-driven algorithms[J]．Energies，2022，15(19)：7432．

[9] XU Weiwei，WENG Jiaming，LOU Boliang，et al．Vulnerability assessment of distributed load shedding algorithm for active distribution power system under denial of service attack[J]．CSEE Journal of Power and Energy Systems，2023，9(6)：2066-2075．

[10] ZHANG Xiaoguang，YANG Guanghong，WASLY S．Man-in-the-middle attack against cyber-physical systems under random access protocol[J]．Information Sciences，2021，576：708-724．

[11] 陈林根，夏少军，冯辉君．不可逆循环的广义热力学动态优化研究进展[J]．中国科学：技术科学，2019，49(11)：1223-1267．
CHEN Lingen，XIA Shaojun，FENG Huijun．Progress in generalized thermodynamic dynamic-optimization of irreversible cycles[J]．Scientia Sinica Technologica，2019，49(11)：1223-1267(in Chinese)．

[12] LI Hao，ZHONG Shengyuan，WANG Yangzhen，et al．New understanding on information's role in the matching of supply and demand of distributed energy system[J]．Energy，2020，206：118036．

[13] 李家熙，王丹，贾宏杰，等．面向可再生能源接入的综合能源系统熵态机理和分析方法[J]．电力系统自动化，2023，47(9)：47-58．
LI Jiaxi，WANG Dan，JIA Hongjie，et al．Entropy state mechanism and analysis method of integrated energy system for integration of renewable energy[J]．Automation of Electric Power Systems，2023，47(9)：47-58(in Chinese)．

[14] 李宜哲，王丹，李家熙，等．面向可再生能源集成的综合能源系统熵态计算模型[J]．电力系统自动化，2024，48(11)：162-172．
LI Yizhe，WANG Dan，LI Jiaxi，et al．Entropy state calculation model of integrated energy system for renewable energy integration[J]．Automation of Electric Power Systems，2024，48(11)：162-172(in Chinese)．

[15] 汤奕，陈倩，李梦雅，等．电力信息物理融合系统环境中的网络攻击研究综述[J]．电力系统自动化，2016，40(17)：59-69．

TANG Yi，CHEN Qian，LI Mengya，et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems，2016，40(17)：59-69(in Chinese).

[16] 张宸赓，许寅，王玥，等. 极寒灾害下电力-天然气耦合系统故障连锁传播过程推演方法[J]. 电网技术，2024，48(10)：4084-4093.
ZHANG Chengeng，XU Yin，WANG Yue，et al. Deduction method for the cascading fault propagation process in integrated power and natural gas systems under extreme cold disasters[J]. Power System Technology，2024，48(10)：4084-4093(in Chinese).

[17] 马静，黄韦博，聂珍存，等. 基于新能源快速调节的孤岛微网弹性恢复策略[J]. 电网技术，2024，48(3)：1103-1113.
MA Jing，HUANG Weibo，NIE Zhencun，et al. Elastic Recovery Strategy of Island Micro-network Based on Rapid Adjustment of New Energy[J]. Power System Technology，2024，48(3)：1103-1113(in Chinese).

[18] 张巍，罗浩. 考虑电力-信息-交通网络耦合的配电网韧性提升策略分析[J]. 电网技术，2024，48(1)：361-372.
ZHANG Wei，LUO Hao. Analysis of Distribution Network Resilience Improvement Strategy Considering Power-information-transportation Network Coupling[J]. Power System Technology，2024，48(1)：361-372(in Chinese).

[19] 李振兴，赵子熠，皮志勇，等. 考虑通信-物理耦合的有源配网故障后协调恢复策略[J]. 电网技术，2024，48(11)：4777-4787.
LI Zhenxing，ZHAO Ziyi，PI Zhiyong，et al. A coordinated recovery strategy for active distribution network faults considering communication physical coupling[J]. Power System Technology，2024，48(11)：4777-4787(in Chinese).

[20] 黄校娟，付蓉，吴英俊，等. 网络攻击下基于贝叶斯图论的配电系统安全分析[J]. 电力建设，2019，40(1)：86-95.
HUANG Xiaojuan，FU Rong，WU Yingjun，et al. Analysis on security of distribution system based on Bayesian graph theory under network attack[J]. Electric Power Construction，2019，40(1)：86-95(in Chinese).

[21] DOYNIKOVA E，KOTENKO I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection[C]//2017 25th Euromicro International Conference on Parallel，Distributed and Network-based Processing (PDP). St. Petersburg：IEEE，2017：346-353.

[22] LIU Hao，SUI Jun. Thermodynamic model for feedback control of systems with uncertain macroscopic states[J]. Chinese Journal of Physics，2019，60：688-694.

[23] 张继国，SINGH V P. 信息熵—理论与应用[M]. 北京：中国水利水电出版社，2012.

[24] 李勇，刘俊勇，刘晓宇，等. 基于潮流熵的电网连锁故障传播元件的脆弱性评估[J]. 电力系统自动化，2012，36(19)：11-16.
LI Yong，LIU Junyong，LIU Xiaoyu，et al. Vulnerability assessment in power grid cascading failures based on entropy of power flow[J]. Automation of Electric Power Systems，2012，36(19)：11-16(in Chinese).

[25] HUANG Zhao，FANG Baling，DENG Jin. Multi-objective optimization strategy for distribution network considering V2G-enabled electric vehicles in building integrated energy system[J]. Protection and Control of Modern Power Systems，2020，5(1)：7.

[26] 江茂泽. 输配气管网的模拟与分析[M]. 北京：石油工业出版社，1995.

[27] LIU Xuezhi，WU Jianzhong，JENKINS N，et al. Combined analysis of electricity and heat networks[J]. Applied Energy，2016，162：1238-1250.

刘佳委

在线出版日期：2025-06-10。
收稿日期：2025-04-15。

作者简介：

刘佳委(2001)，男，硕士研究生，研究方向为综合能源系统分析等，E-mail：liujiawei0514@tju.edu.cn；

王丹(1981)，男，副教授，博士生导师，通信作者，研究方向为综合能源系统规划、运行控制、能源市场交易等，E-mail：wangdantjuee@tju.edu.cn。

（责任编辑　徐梅）

附录 A

网络攻击图的连接方式如图 A1 所示。本文定义的攻击图为 $AG=(S,B,P)$，其中 S 代表属性状态节点集合，为各类设备节点；B 为攻击图有向边集合，两个设备节点间的有向边即表示信息攻击传播的路径；P 为单步攻击成功概率集合，表示状态节点转移的概率。

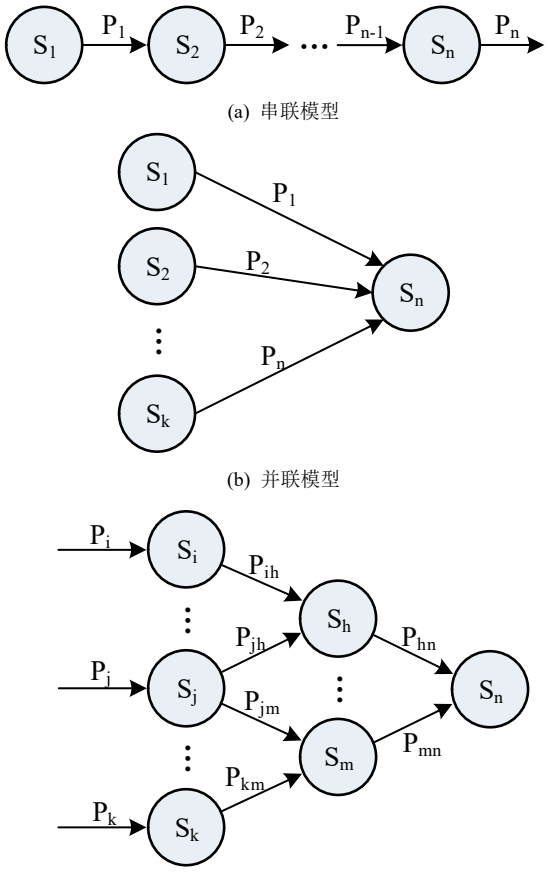


图 A1　网络攻击图连接方式示意图

Fig. A1　Network attack diagram of the connection mode

串联模型攻击成功的概率总值为

$$P_{\text{series}}^{\text{total}}=\prod_{i=1}^{n}P_i \tag{A1}$$

式中：P_i 为攻击路径上单步攻击 i 成功的概率。

并联模型攻击成功的概率总值为

$$P_{\text{parallel}}^{\text{total}}=1-\prod_{i=1}^{n}(1-P_i) \tag{A2}$$

对于信息攻击成功作用于串并联混合模型的概率，则需要遍历从初始状态节点到目标状态节点的所有攻击路径，每条路径都按串联模型处理，其概率总值为

$$P_{\text{s\&p}}^{\text{total}}=\sum_{t=1}^{n}P_t \tag{A3}$$

式中：P_t 为串联模型下攻击路径 t 的成功攻击概率总值。

FTU、DTU、RTU 等传输与控制终端作为网络攻击者常选择的攻击入口，由于设备各自承担功能不同、使用环境不同，导致其网络攻击下的防护功能也不尽相同，被网络攻击者选为攻击入口的概率也各不相同，本文对不同设备作为攻击入口的概率赋值如附录 C 表 C1 所示。

网络攻击是一个多级信息传递过程，攻击者实施单步攻击的成功与否，不仅与设备节点自身的固有漏洞相关，还与攻击者的能力密切相关。参照通用漏洞评分系统(Common Vulnerability Scoring System，CVSS)[21]来计算漏洞被利用的概率，计算公式为

$$P_i^1=AV_i*w_1+AC_i*w_2+AU_i*w_3+RL_i*w_4+EX_i*w_5 \tag{A4}$$

式中：AV_i 、AC_i 、AU_i 、RL_i 分别为设备 i 的访问向量、访问复杂度、认证次数度量、漏洞的修复程度指标，具体等级与评分如附录 C 表 C2 所示；EX_i 为设备 i 漏洞的随时间暴露程度；w_1-w_5 为相应指标的权重值，具体赋值如附录 C 表 C3 所示。

EX_i 可用帕累托分布计算：

$$EX_i=1-\left(\frac{\beta}{t_i}\right)^{\alpha} \tag{A5}$$

式中：α 、β 为帕累托分布参数，本文取 α =0.25，β =0.05；t_i 为漏洞 i 的发布时长，本文取 t_i =30。

攻击者在掌握了设备漏洞的基本属性后，可以成功利用该漏洞发动攻击的概率值计算公式为

$$P_i^2=\frac{k}{N_i}*\frac{1}{1+e^{-\left\{\log_2\left[0.4*(M_i+1)\right]-5\right\}}} \tag{A6}$$

式中：k 表示攻击者对系统的掌握程度，$k\in[0,1]$；N_i 为设备 i 的漏洞总数；M_i 为攻击者对设备 i 的攻击次数。

综上，设备节点 i 被成功攻击的概率为

$$P_i=P_i^1*P_i^2 \tag{A6}$$

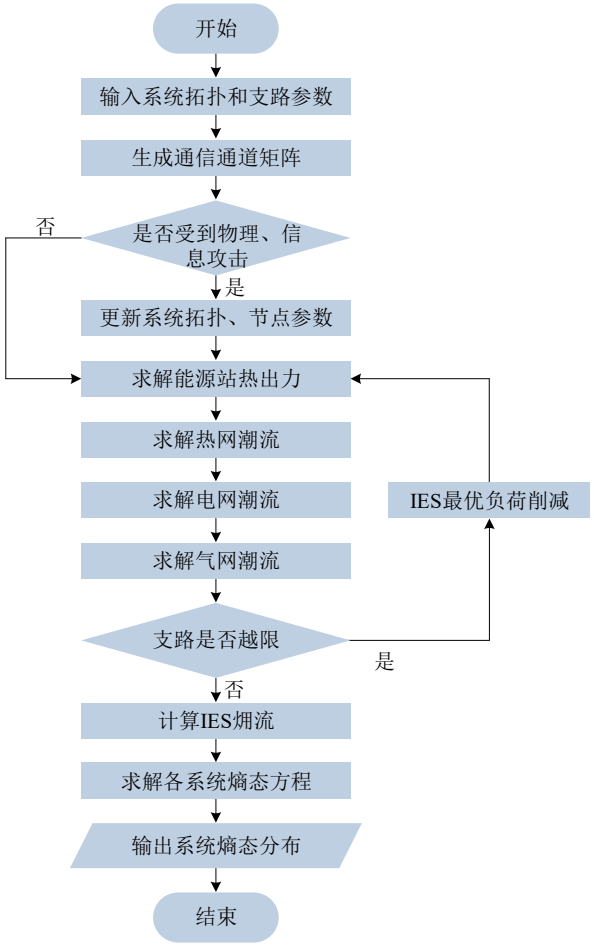


图 A2　网络攻击下 IECPS 熵态计算流程

Fig. A2　Flow chart of IECPS entropy increase calculation under network attack

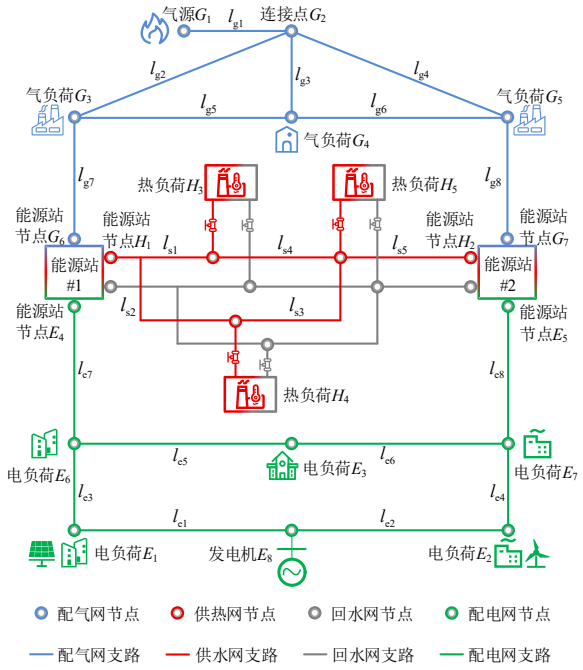


图 A3　算例测试系统示意图

Fig. A3　Schematic diagram of the test case system

该系统包含 3 个能源子系统：8 节点电力系统、7 节点天然气系统和 5 节点热力系统，配备两个能源站。IES烟流模型和熵态模型的环境温度设为 10℃。8 节点配电网参数基于 IEEE33 节点系统[25]修改，7 节点中压配气网参数基于 5 节点天然气系统数据[26]进行修改，气源气压为 0.5MPa，天然气的热值和理论燃烧温度分别为45.75MJ/m^{3}和1973℃。区域热力系统的相关参数基于 3 节点典型区域热力网络[27]数据进行修改。两个能源站为供热系统提供热能，热源出水温度设为 100℃，负荷出水温度为 50℃。

算例配置的 2 个典型能源站中，ES1 配备了一台热电联供机组和一台燃气锅炉，能源转化效率分别为$\eta_{g2e}^{CHP}=0.3$、$\eta_{g2h}^{CHP}=0.4$和$\eta_{g2h}^{GB}=0.85$。ES2 配备了一台燃气锅炉和一台电锅炉，能源转化效率分别为$\eta_{g2h}^{GB}=0.85$和$\eta_{e2h}^{EB}=0.95$。针对源荷不确定性导致的信息学等效热力学熵增，本文基于源荷全年逐时数据，以文献[13]中弱预测场景为例，构建源荷熵态模型。

附录 B

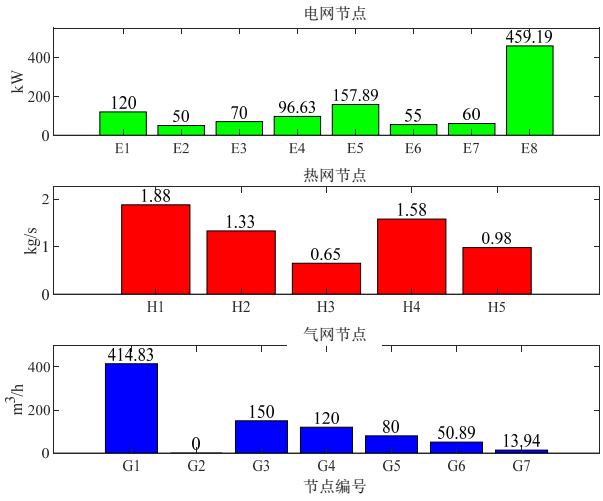


图 B1　场景一无网络攻击下系统节点注入/输出能流

Fig. B1　System nodes inject/output energy flows in no network attack

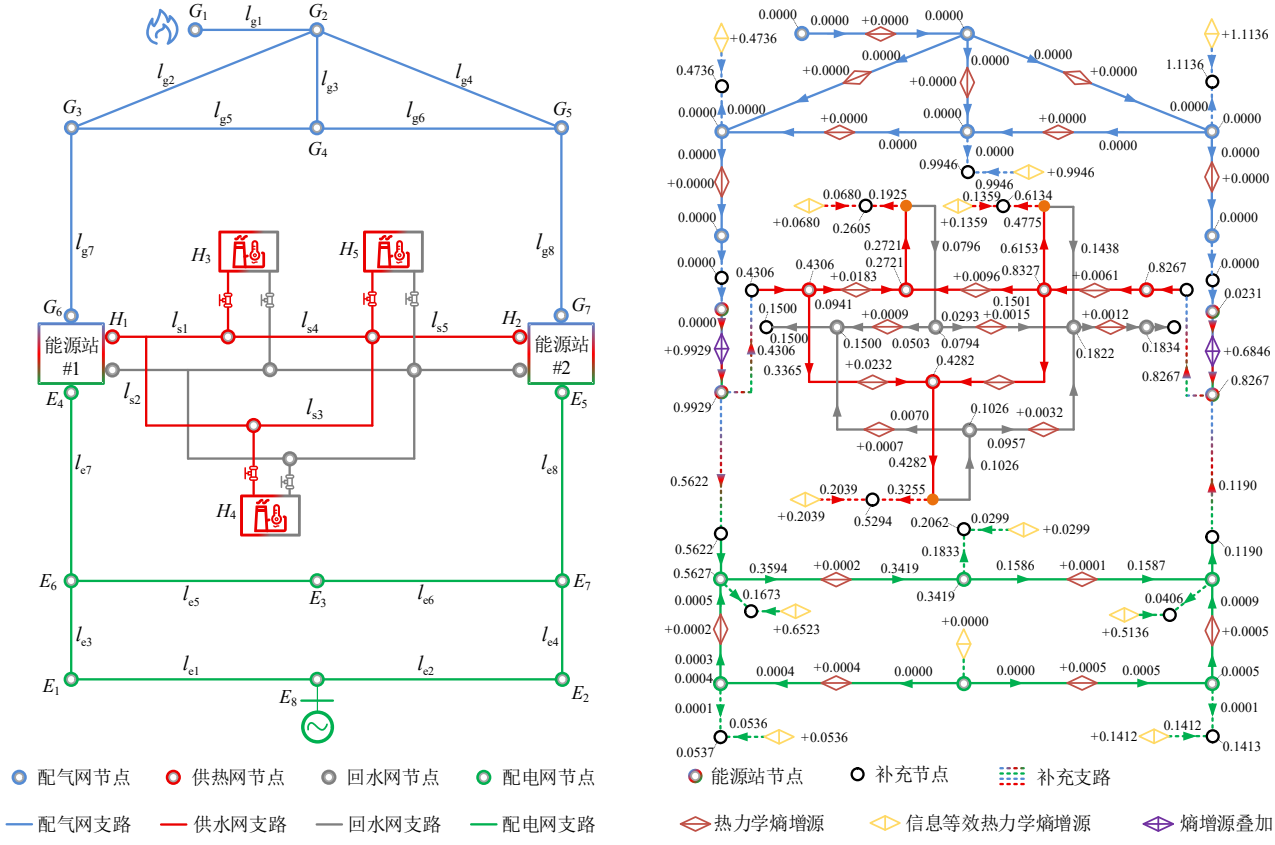


图 B2　场景一无网络攻击下系统物理拓扑和熵态图

Fig. B2　The physical topology and entropy state diagram of the system under no network attack

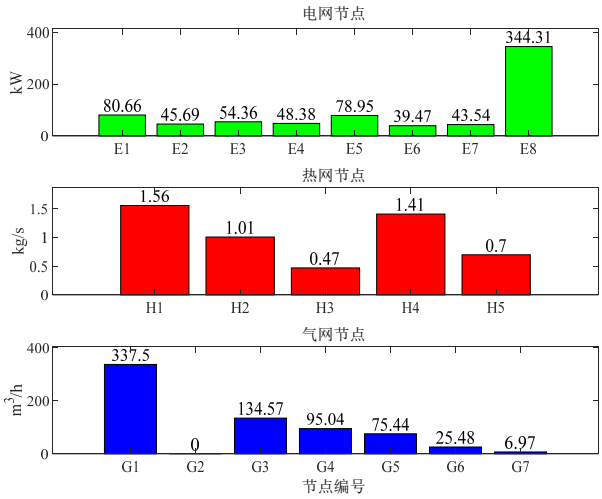


图 B3　场景二中强攻击场景下系统节点注入/输出能流

Fig. B3　System nodes inject/output energy flows in strong attack scenario

相较于场景一的稳态运行方式，在该场景下，配电网负荷节点 E_1 切除负荷 39.34kW，负荷节点 E_2 切除负荷 4.31kW，负荷节点 E_3 切除负荷 15.64kW，能源站节点 E_5 切除负荷 78.94kW，负荷节点 E_6 切除负荷 15.53kW，负荷节点 E_7 切除负荷 16.46kW。气负荷节点 G_3 切除负荷 15.43m^3/h，负荷节点 G_4 切除负荷 24.96m^3/h，负荷节点 G_5 切除负荷 4.56m^3/h，能源站节点 G_6 切除负荷 25.41m^3/h，能源站节点 G_7 切除负荷 6.97m^3/h。热负荷节点 H_3 切除负荷 0.18kg/s，负荷节点 H_4 切除负荷 0.17kg/s，负荷节点 H_5 切除负荷 0.28kg/s。

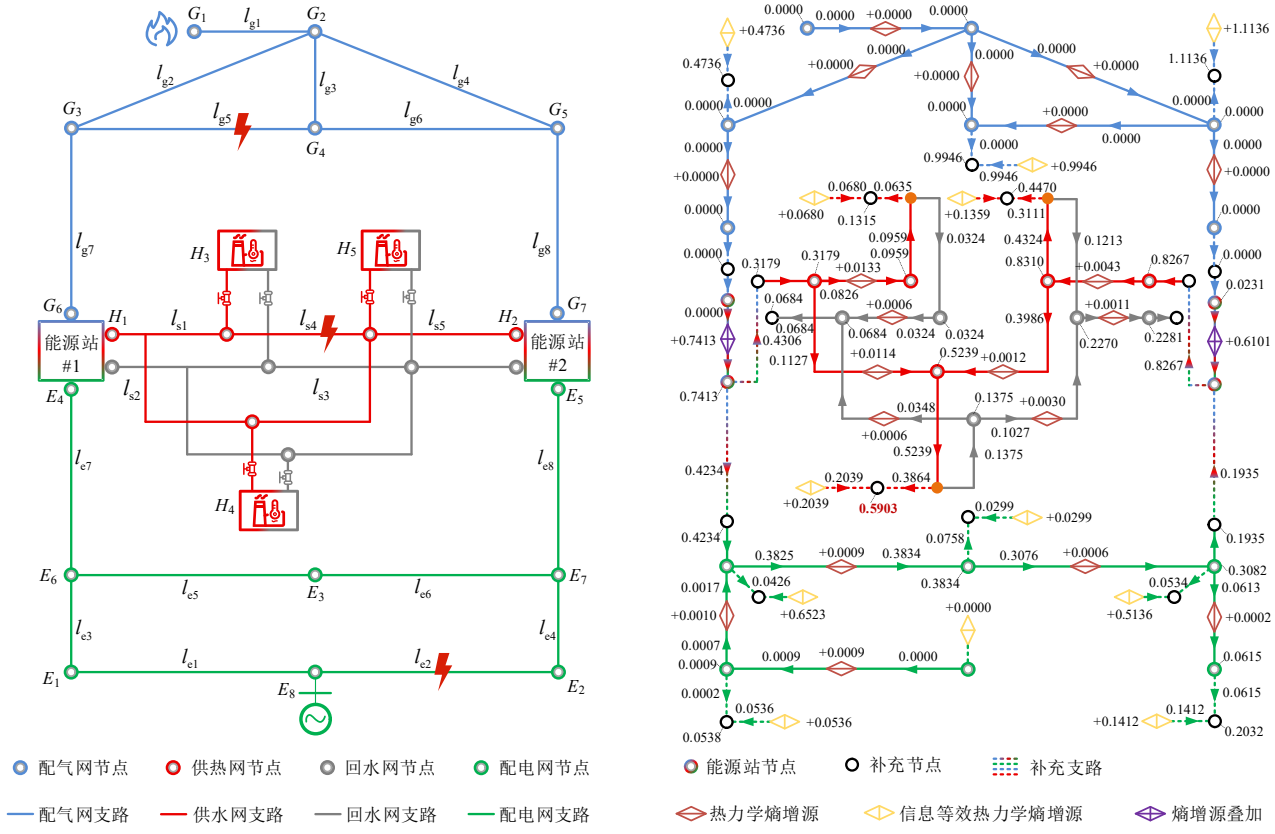


图 B4　场景二中强攻击场景下熵态结果示意图

Fig. B4　Schematic diagram of entropy state results in strong attack scenario

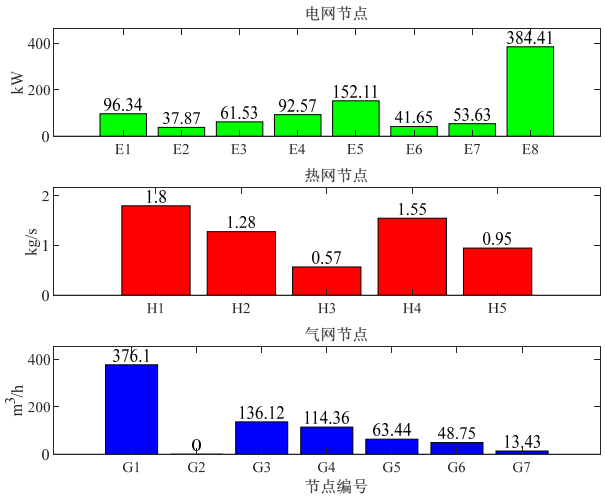


图 B5　场景二中弱攻击场景下系统节点注入/输出能流

Fig. B5　System nodes inject/output energy flows in weak attack scenario

配电网负荷节点 E_1 切除负荷 23.66kW，负荷节点 E_2 切除负荷 12.13kW，负荷节点 E_3 切除负荷 8.47kW，能源站节点 E_5 切除负荷 5.78kW，负荷节点 E_6 切除负荷 13.25kW，负荷节点 E_7 切除负荷 6.37kW。配气网负荷节点 G_3 切除负荷 13.88m^3/h，负荷节点 G_4 切除负荷 5.64m^3/h，负荷节点 G_5 切除负荷 16.56m^3/h，能源站节点 G_6 切除负荷 2.14m^3/h，能源站节点 G_7 切除负荷 0.51m^3/h。热负荷节点 H_3 切除负荷 0.08kg/s，负荷节点 H_4 切除负荷 0.03kg/s，负荷节点 H_5 切除负荷 0.03kg/s。在该场景下，由于网络攻击作用于部分支路所在的信息网络后，将信息采集装置采集的正常潮流信息篡改为越限状态，根据 2.3.3 节建立的网络攻击熵增计算模型求解信息攻击熵增。气网管道 l_{g5} 两端节点 G_3、G_4 分别承担 0.0113kW/K 的信息攻击熵增；热网管道 l_{s4} 两端节点 H_3、H_4 分别承担 0.1501kW/K 的信息攻击熵增；电网线路 l_{e2} 两端节点 E_2、E_8 分别承担 0.0023kW/K 的信息攻击熵增。由于线路受网络攻击产生的信息攻击熵增均在网络中流动，且遵循节点熵增分配定律。

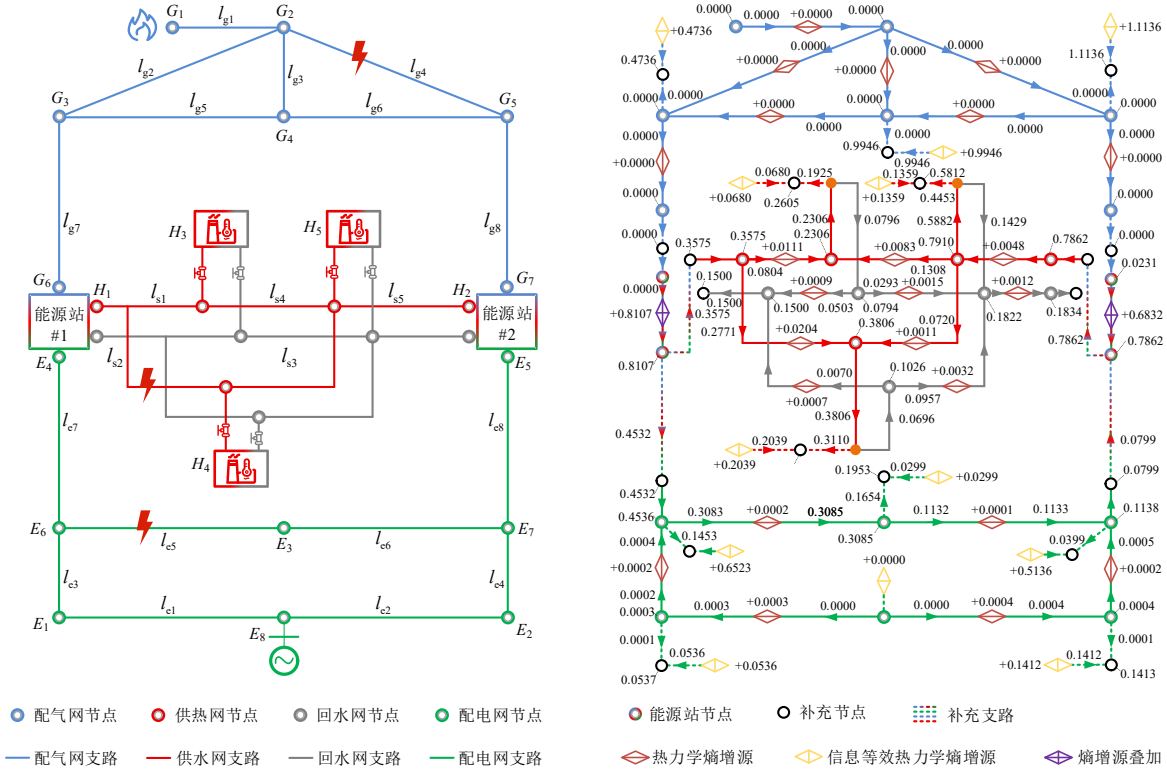


图 B6　场景二弱攻击场景下熵态结果示意图

Fig. B6　Schematic diagram of entropy state results in weak attack scenario

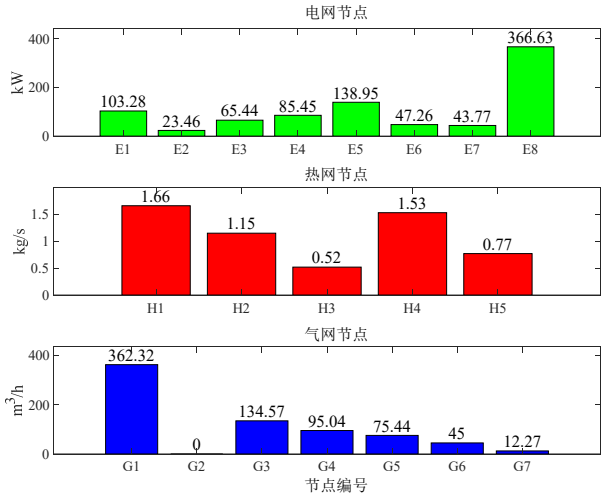


图 B7　场景三受攻击后系统节点注入/输出能流

Fig. B7　System nodes inject/output energy flows in scenario 3

配电网负荷节点 E_1 切除负荷 16.72kW，负荷节点 E_2 切除负荷 26.54kW，负荷节点 E_3 切除负荷 4.56kW，能源站节点 E_5 切除负荷 5.78kW，负荷节点 E_6 切除负荷 18.94kW，负荷节点 E_7 切除负荷 16.23kW。配气网负荷节点 G_3 切除负荷 15.43m^3/h，负荷节点 G_4 切除负荷 24.96m^3/h，负荷节点 G_5 切除负荷 4.56m^3/h，能源站节点 G_6 切除负荷 5.89m^3/h，能源站节点 G_7 切除负荷 1.67m^3/h。热负荷节点 H_3 切除负荷 0.14kg/s，负荷节点 H_4 切除负荷 0.05kg/s，负荷节点 H_5 切除负荷 0.21kg/s。

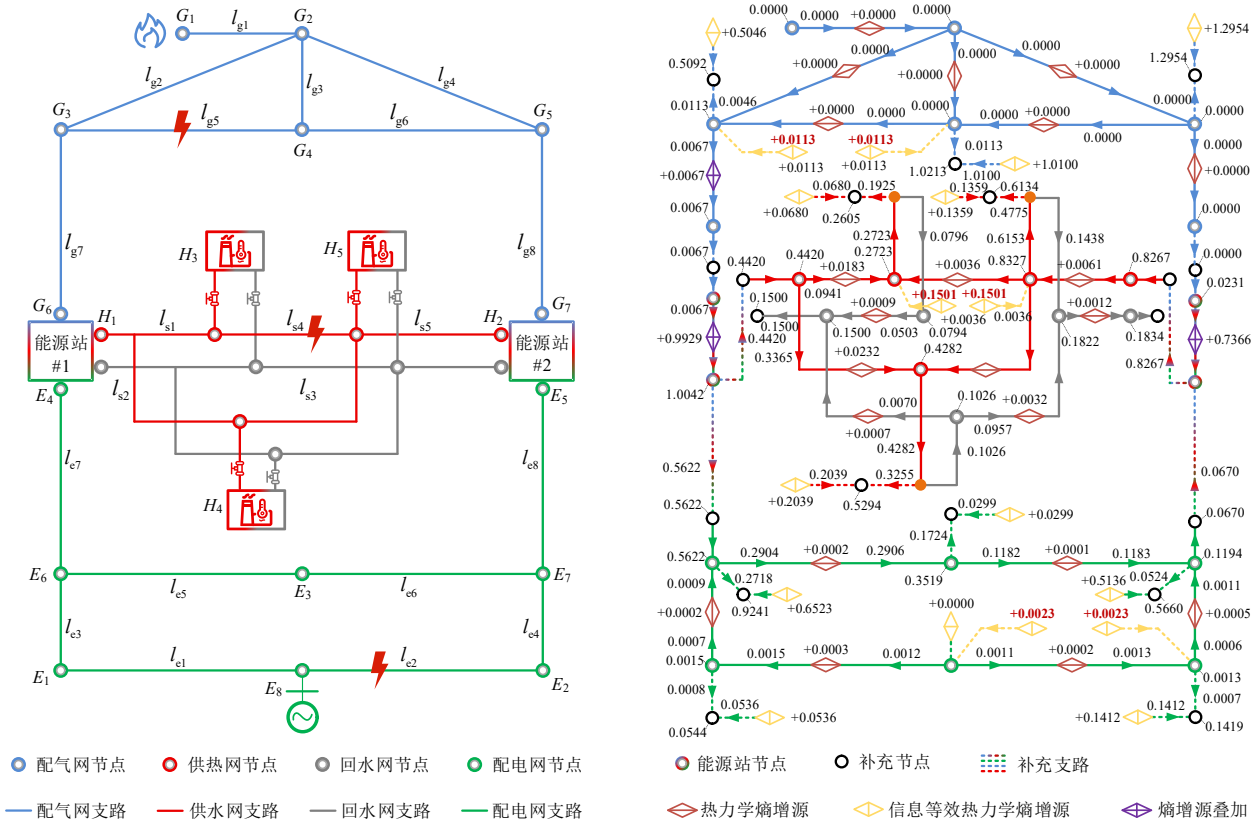


图 B8　场景三受攻击后熵态结果示意图

Fig. B8　Schematic diagram of system entropy state results in scenario 3

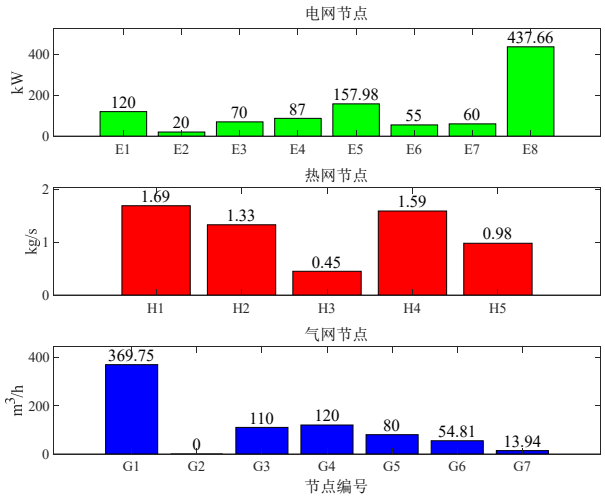


图 B9　场景四受攻击后系统节点注入/输出能流

Fig. B9　System nodes inject/output energy flows in scenario 4

在该场景下，网络攻击作用于部分节点所在信息网络，根据 2.3.3 节建立的网络攻击熵增计算模型求解节点信息攻击熵增。电网节点 E_2 产生信息攻击熵增 0.0427kW/K；气网节点 G_3 产生信息攻击熵增 0.0985kW/K；热网节点 H_3 产生信息攻击熵增 0.1427kW/K。

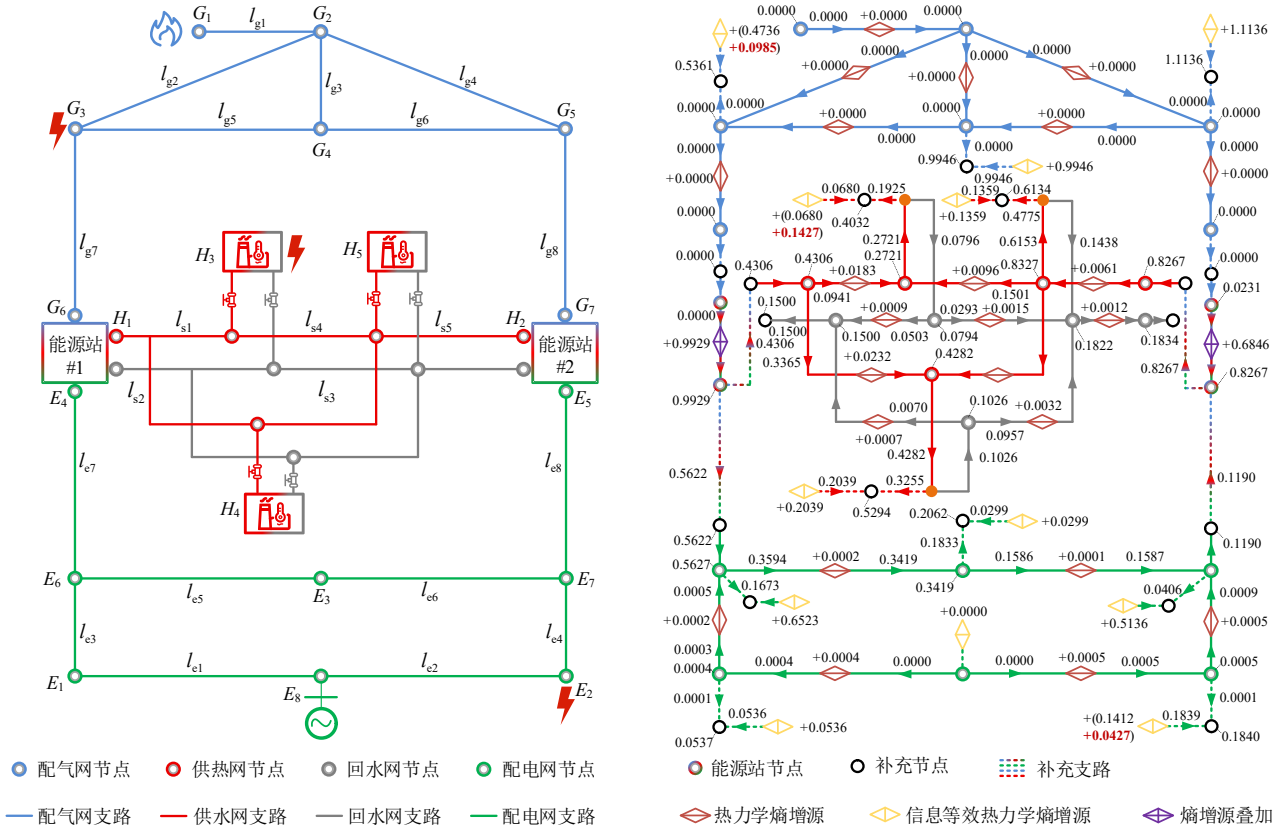


图 B10　场景四受攻击后熵态结果示意图

Fig. B10　Schematic diagram of system entropy state results in scenario 4

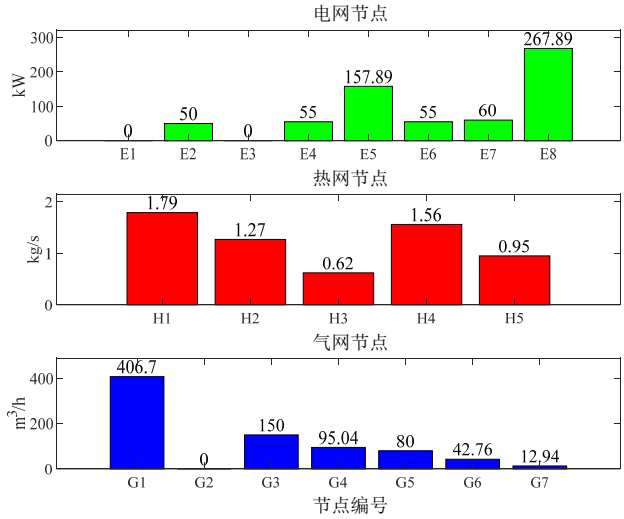
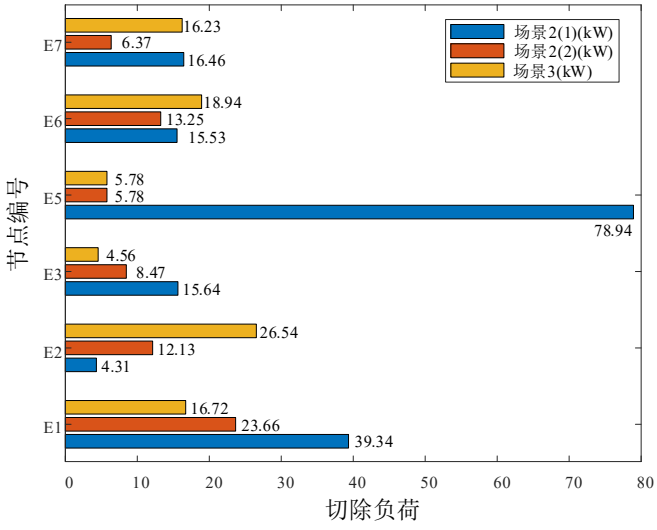
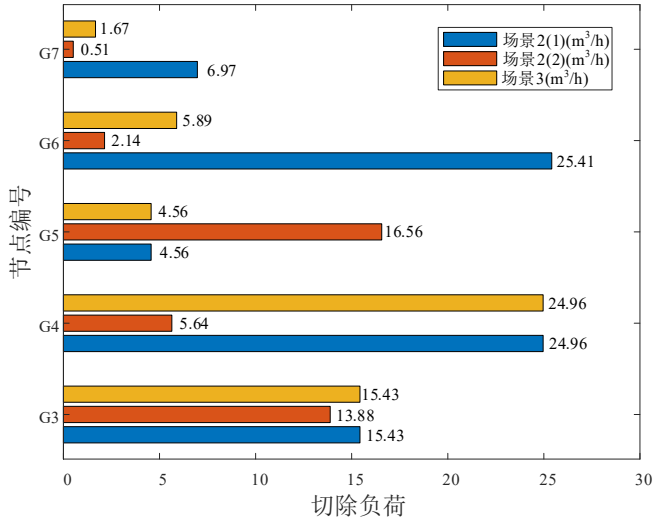


图 B11　场景五受攻击后系统节点注入/输出能流

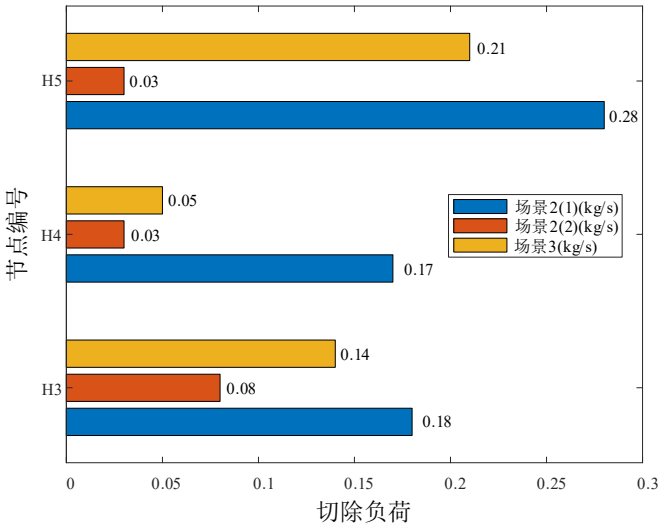
Fig. B11　System nodes inject/output energy flows in scenario 5



(a) 场景 2、3 下电网节点切负荷情况



(b) 场景 2、3 下气网节点切负荷情况



(c) 场景 2、3 下热网节点切负荷情况

图 B12　场景 2-3 下系统切负荷情况

Fig. B12　Load reduction in Scenario 2-3

附录 C

表 C1　不同设备作为攻击入口的概率赋值

Table C1　Probability assignment of different devices as attack entry points

节点	采集/控制设备	攻击概率	通信设备	攻击概率	线路	采集/控制设备	攻击概率	通信设备	攻击概率
E_1	TTU	0.3	DTU	0.2	l_{e1}	FTU	0.5	DTU	0.2
E_2	RTU	0.2	DTU	0.2	l_{e2}	FTU	0.5	DTU	0.2
E_3	RTU	0.2	DTU	0.2	l_{e3}	FTU	0.5	DTU	0.2
E_4	RTU	0.2	DTU	0.2	l_{e4}	FTU	0.5	DTU	0.2
E_5	RTU	0.2	DTU	0.2	l_{e5}	FTU	0.5	DTU	0.2
E_6	RTU	0.2	DTU	0.2	l_{e6}	FTU	0.5	DTU	0.2
E_7	RTU	0.2	DTU	0.2	l_{e7}	FTU	0.5	DTU	0.2
E_8	RTU	0.2	DTU	0.2	l_{e8}	FTU	0.5	DTU	0.2
G_1	RTU	0.2	DTU	0.2	l_{g1}	RTU	0.2	DTU	0.2
G_2	RTU	0.2	DTU	0.2	l_{g2}	RTU	0.2	DTU	0.2
G_3	RTU	0.2	DTU	0.2	l_{g3}	RTU	0.2	DTU	0.2
G_4	RTU	0.2	DTU	0.2	l_{g4}	RTU	0.2	DTU	0.2
G_5	RTU	0.2	DTU	0.2	l_{g5}	RTU	0.2	DTU	0.2
G_6	RTU	0.2	DTU	0.2	l_{g6}	RTU	0.2	DTU	0.2
G_7	RTU	0.2	DTU	0.2	l_{g7}	RTU	0.2	DTU	0.2
H_1	RTU	0.2	DTU	0.2	l_{g8}	RTU	0.2	DTU	0.2
H_2	RTU	0.2	DTU	0.2	l_{h1}	RTU	0.2	DTU	0.2
H_3	RTU	0.2	DTU	0.2	l_{h2}	RTU	0.2	DTU	0.2
H_4	RTU	0.2	DTU	0.2	l_{h3}	RTU	0.2	DTU	0.2
H_5	RTU	0.2	DTU	0.2	l_{h4}	RTU	0.2	DTU	0.2
					l_{h5}	RTU	0.2	DTU	0.2

表 C2　CVSS 等级与评分对应表

Table C2　Corresponding table of CVSS grades and scores

指标名称	等级	评分
访问向量(*AV*)	本地访问	0.395
	邻近网络访问	0.646
	远程网路访问	1.0
访问复杂度(*AC*)	高	0.35
	中	0.61
	低	0.71
认证(*AU*)	多次认证	0.45
	单次认证	0.56
	不需要认证	0.704
补丁修复等级(*RL*)	官方补丁	0.87

临时补丁	0.9
临时解决方案	0.95
无补丁	1

表 C3　漏洞被利用的概率计算指标赋值

Table C3　Probability calculation and indicator assignment of vulnerability exploitation

指标	赋值
w_1	0.138
w_2	0.169
w_2	0.200
w_2	0.231
w_2	0.263

表 C4　不同场景下网络攻击成功概率

Table C4　Probability of successful network attacks under different scenarios

场景	网络攻击路径	攻击成功概率
场景一	/	/
场景二	/	/
场景三	l_{e2} FTU→DTU→通信汇集子站→前置机→主站控制中心	0.00874
	l_{g5} RTU→DTU→通信汇集子站→前置机→主站控制中心	0.00945
	l_{h4} RTU→DTU→通信汇集子站→前置机→主站控制中心	0.00945
场景四	主站控制中心→前置机→通信汇集子站→DTU→ E_2 RTU	0.00362
	主站控制中心→前置机→通信汇集子站→DTU→ G_3 RTU	0.00362
场景五	主站控制中心→前置机→通信汇集子站→DTU→ H_3 RTU	0.00362
	主站控制中心→前置机→通信汇集子站→DTU→ l_{e4} FTU	0.00417

表 C5　场景设置情况及部分结果表

Table C5　Scenario Settings and partial results table

场景	攻击类型	攻击目标	攻击方式	信息攻击熵增 (kW/K)	攻击后的信息攻击熵增源形式	潮流分布熵等效热力学熵增 (kW/K)	潮流转移熵等效热力学熵增 (kW/K)	网络攻击对能源网络造成的影响 开断管线	电负荷损失量(kW) / 百分比	气负荷损失量(m^3/h) / 百分比	热负荷损失量(kg/s) / 百分比
场景一	无网络攻击	/	/	/	/	/	/	/	/	/	/
场景二(强攻击)	物理攻击	l_{e2} l_{g5} l_{s4} 线路或管道	物理破坏至管线永久性断开	/	/	0.1266	0.2874	l_{e2} l_{g5} l_{s4} 线路或管道	170.22/ 33.19%	36.07/ 8.70%	0.63/ 19.63%
场景二(弱攻击)	物理攻击	l_{e5} l_{g4} l_{s2} 线路或管道	物理破坏至管线能流承载能力下降	/	/	0.1064	/	/	69.66/ 13.58%	38.73/ 9.34%	0.14/ 4.36%
场景三	信息攻击	l_{e2} FTU l_{g5} RTU l_{s4} RTU	FDI	E_2 :0.0023 E_8 :0.0023 G_3 :0.0113 G_4 :0.0113 H_3 :0.1501 H_5 :0.1501		0.1621	/	/	88.77/ 17.31%	52.51/ 12.66%	0.40/ 12.46%
场景四	信息攻击	E_2 RTU G_3 RTU H_3 RTU	FDI	E_4 :0.0427 G_3 :0.0985 H_3 :0.1427		0.0924	/	/	30/ 5.85%	40/ 9.26%	0.20/ 6.23%
场景五	先物理后信息协同攻击	l_{e5} 线路对应的控制中心部分	DoS	E_6 :0.1215 E_7 :0.1215		0.1251	0.3565	l_{e1} l_{e5} l_{e6} 线路	190/ 37.04%	29.12/ 7.02%	0.23/ 7.17%

注：场景二、场景三的控制中心切负荷策略如附录 B 图 B12 所示

表 C6　场景一无网络攻击下系统能流分布

Table C6　System energy flow distribution in Scenario 1 without network attacks

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/(kW)	线路	有功/kW	有功损耗/kW
E_1	12.66∠0	120.00	l_{e1}	218.26	5.07
E_2	12.66∠7.06×10^{-5}	50.00	l_{e2}	226.26	9.60

E_3	12.64∠2.36×10^{-4}	70.00	l_{e3}	98.26	6.42
E_4	12.63∠4.03×10^{-4}	96.63	l_{e4}	176.26	13.48
E_5	12.64∠4.09×10^{-4}	157.89	l_{e5}	130.60	1.42
E_6	12.66∠1.52×10^{-4}	55.00	l_{e6}	60.60	0.47
E_7	12.65∠3.65×10^{-4}	60.00	l_{e7}	96.63	1.45
E_8	12.64∠4.01×10^{-4}	459.19	l_{e8}	157.89	5.02

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压/(MPa)	气流率/(m^3/h)	功率/kW	管道	起点	终点	气流率/(m^3/h)
G_1	0.5	414.83	/	l_{g1}	G_1	G_2	414.83
G_2	0.5	0	/	l_{g2}	G_2	G_3	148.51
G_3	0.5	150.00	1625.13	l_{g3}	G_2	G_4	136.37
G_4	0.5	120.00	1300.10	l_{g4}	G_2	G_5	129.95
G_5	0.5	80.00	866.74	l_{g5}	G_3	G_4	52.38
G_6	0.5	42.76	463.27	l_{g6}	G_4	G_5	36.01
G_7	0.5	13.94	151.02	l_{g7}	G_3	G_6	50.89
				l_{g8}	G_5	G_7	13.94

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.88	377.62	l_{s1}	H_1	H_3	0.41
H_2	1.33	267.16	l_{s2}	H_1	H_4	1.47
H_3	0.65	130.60	l_{s3}	H_5	H_4	0.11
H_4	1.58	317.46	l_{s4}	H_5	H_3	0.24
H_5	0.98	196.90	l_{s5}	H_2	H_5	1.33

表 C7　场景 2 中强攻击场景下系统能流分布

Table C7　System energy flow distribution in a strong attack scenario in Scenario 2

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/kW	线路	有功/kW	有功损耗/kW
E_1	12.66∠0	80.66	l_{e1}	−328.47	0.24
E_2	12.61∠6.44×10^{-4}	45.69	l_{e2}	/	/
E_3	12.64∠4.57×10^{-4}	54.36	l_{e3}	247.81	5.38
E_4	12.62∠4.74×10^{-4}	48.38	l_{e4}	−45.69	3.45
E_5	12.64∠3.55×10^{-4}	78.95	l_{e5}	−228.18	1.37
E_6	12.66∠1.52×10^{-4}	39.47	l_{e6}	173.82	0.70
E_7	12.65∠5.31×10^{-4}	43.54	l_{e7}	51.51	7.49
E_8	12.64∠5.23×10^{-4}	344.31	l_{e8}	−78.95	0.80

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压/(MPa)	气流率/(m^3/h)	功率/kW	管道	起点	终点	气流率/(m^3/h)
G_1	0.5	337.50	/	l_{g1}	G_1	G_2	337.50
G_2	0.5	0	/	l_{g2}	G_2	G_3	192.76
G_3	0.5	134.57	1709.06	l_{g3}	G_2	G_4	107.52
G_4	0.5	95.04	1207.38	l_{g4}	G_2	G_5	106.42
G_5	0.5	75.44	958.30	l_{g5}	G_3	G_4	/
G_6	0.5	25.48	323.77	l_{g6}	G_4	G_5	12.48
G_7	0.5	6.97	88.45	l_{g7}	G_3	G_6	42.76
				l_{g8}	G_5	G_7	13.94

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.56	313.55	l_{s1}	H_1	H_3	0.835
H_2	1.01	202.93	l_{s2}	H_1	H_4	/
H_3	0.47	94.43	l_{s3}	H_5	H_4	1.81
H_4	1.41	283.40	l_{s4}	H_5	H_3	0.71
H_5	0.70	140.64	l_{s5}	H_2	H_5	2.21

表 C8　场景 2 中弱攻击场景下系统能流分布

Table C8　System energy flow distribution in the weak attack scenario in Scenario 2

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/kW	线路	有功/kW	有功损耗/kW
E_1	12.66∠0	96.34	l_{e1}	177.87	0.02

E_2	12.66∠7.06×10^{-5}	37.87	l_{e2}	195.69	0.074
E_3	12.64∠2.36×10^{-4}	61.53	l_{e3}	81.53	6.02
E_4	12.63∠4.03×10^{-4}	92.57	l_{e4}	158.09	3.25
E_5	12.64∠4.09×10^{-4}	152.11	l_{e5}	125.09	1.22
E_6	12.66∠1.52×10^{-4}	41.65	l_{e6}	63.56	0.18
E_7	12.65∠3.65×10^{-4}	53.63	l_{e7}	92.57	8.95
E_8	12.64∠4.01×10^{-4}	384.41	l_{e8}	152.11	2.48

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压/(MPa)	气流率/(m^3/h)	功率/kW	管道	起点	终点	气流率/(m^3/h)
G_1	0.5	376.10	/	l_{g1}	G_1	G_2	376.10
G_2	0.5	0	/	l_{g2}	G_2	G_3	135.84
G_3	0.5	136.12	1474.76	l_{g3}	G_2	G_4	124.23
G_4	0.5	114.36	1239.07	l_{g4}	G_2	G_5	116.40
G_5	0.5	63.44	687.27	l_{g5}	G_3	G_4	49.04
G_6	0.5	48.75	528.27	l_{g6}	G_4	G_5	39.17
G_7	0.5	13.43	145.53	l_{g7}	G_3	G_6	48.75
				l_{g8}	G_5	G_7	13.43

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.80	361.67	l_{s1}	H_1	H_3	0.36
H_2	1.28	257.19	l_{s2}	H_1	H_4	1.44
H_3	0.57	114.53	l_{s3}	H_5	H_4	0.11
H_4	1.55	311.43	l_{s4}	H_5	H_3	0.20
H_5	0.95	190.88	l_{s5}	H_2	H_5	1.28

表 C9　场景 3 受攻击后系统能流分布

Table C9　Energy flow distribution of the attacked system in Scenario 3

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/kW	线路	有功/kW	有功损耗/kW
E_1	12.66∠0	103.28	l_{e1}	183.31	0.13
E_2	12.65∠4.13×10^{-5}	23.46	l_{e2}	174.05	0.11
E_3	12.65∠3.47×10^{-4}	65.44	l_{e3}	80.03	2.36
E_4	12.63∠2.56×10^{-4}	85.45	l_{e4}	150.59	3.77
E_5	12.65∠3.66×10^{-4}	138.95	l_{e5}	111.34	1.24
E_6	12.66∠2.33×10^{-4}	47.26	l_{e6}	45.90	0.26
E_7	12.65∠3.16×10^{-4}	43.77	l_{e7}	85.45	4.23
E_8	12.64∠2.68×10^{-4}	366.63	l_{e8}	138.95	2.11

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压/(MPa)	气流率/(m^3/h)	功率/kW	管道	起点	终点	气流率/(m^3/h)
G_1	0.5	362.32	/	l_{g1}	G_1	G_2	332.55
G_2	0.5	0	/	l_{g2}	G_2	G_3	120.997
G_3	0.5	134.57	1458.05	l_{g3}	G_2	G_4	108.12
G_4	0.5	95.04	1029.68	l_{g4}	G_2	G_5	103.46
G_5	0.5	75.44	817.37	l_{g5}	G_3	G_4	48.89
G_6	0.5	45.00	487.54	l_{g6}	G_4	G_5	27.21
G_7	0.5	12.27	132.92	l_{g7}	G_3	G_6	45.00
				l_{g8}	G_5	G_7	12.27

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.66	333.54	l_{s1}	H_1	H_3	0.30
H_2	1.15	231.06	l_{s2}	H_1	H_4	1.36
H_3	0.52	104.48	l_{s3}	H_5	H_4	0.17
H_4	1.53	307.46	l_{s4}	H_5	H_3	0.21
H_5	0.77	154.71	l_{s5}	H_2	H_5	1.15

表 C10　场景 4 受攻击后系统能流分布

Table C10　Energy flow distribution of the attacked system in Scenario 4

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/kW	线路	有功/kW	有功损耗/kW

E_1	12.66∠0	120.00	l_{e1}	223.15	0.55
E_2	$12.65\angle 2.87\times10^{-5}$	20.00	l_{e2}	201.61	0.98
E_3	$12.65\angle 1.77\times10^{-4}$	70.00	l_{e3}	13.15	0.04
E_4	$12.63\angle 5.43\times10^{-4}$	86.99	l_{e4}	181.61	1.44
E_5	$12.65\angle 1.72\times10^{-4}$	157.89	l_{e5}	125.76	0.74
E_6	$12.66\angle 2.99\times10^{-4}$	55.00	l_{e6}	55.76	0.23
E_7	$12.65\angle 3.47\times10^{-4}$	60.00	l_{e7}	86.99	1.68
E_8	$12.64\angle 9.45\times10^{-5}$	437.66	l_{e8}	157.89	1.54

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压/(MPa)	气流率/(m^3/h)	功率/kW	管道	起点	终点	气流率/(m^3/h)
G_1	0.5	369.75	/	l_{g1}	G_1	G_2	369.75
G_2	0.5	0	/	l_{g2}	G_2	G_3	127.39
G_3	0.5	110.00	1191.76	l_{g3}	G_2	G_4	123.01
G_4	0.5	120.00	1300.10	l_{g4}	G_2	G_5	119.35
G_5	0.5	80.00	866.74	l_{g5}	G_3	G_4	28.43
G_6	0.5	45.81	496.37	l_{g6}	G_4	G_5	25.41
G_7	0.5	13.94	151.02	l_{g7}	G_3	G_6	45.81
				l_{g8}	G_5	G_7	13.94

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.69	339.78	l_{s1}	H_1	H_3	0.26
H_2	1.33	267.16	l_{s2}	H_1	H_4	1.43
H_3	0.45	90.41	l_{s3}	H_5	H_4	1.16
H_4	1.59	319.48	l_{s4}	H_5	H_3	0.18
H_5	0.98	196.90	l_{s5}	H_2	H_5	1.33

表 C11　场景 5 受攻击后系统能流分布

Table C11　Energy flow distribution of the attacked system in Scenario 5

电力节点电压及功率			电力系统潮流分布		
节点	电压/(kV∠rad)	有功/kW	线路	有功/kW	有功损耗/kW
E_1	12.66∠0	0.00	l_{e1}	/	/
E_2	$12.65\angle 0.47\times10^{-4}$	50.00	l_{e2}	201.61	0.98
E_3	$12.66\angle 1.03\times10^{-4}$	0.00	l_{e3}	/	/
E_4	$12.64\angle 6.48\times10^{-5}$	55.00	l_{e4}	181.61	1.44
E_5	$12.65\angle 1.33\times10^{-4}$	157.89	l_{e5}	/	/
E_6	$12.64\angle 1.29\times10^{-4}$	55.00	l_{e6}	/	/
E_7	$12.64\angle 6.56\times10^{-5}$	60.00	l_{e7}	86.99	1.68
E_8	$12.64\angle 9.45\times10^{-5}$	267.89	l_{e8}	157.89	1.54

天然气节点气压、气流率、功率				天然气管道气流率			
节点	气压(MPa)	气流率(m^3/h)	功率/kW	管道	起点	终点	气流率(m^3/h)
G_1	0.5	406.70	/	l_{g1}	G_1	G_2	406.70
G_2	0.5	0.00	/	l_{g2}	G_2	G_3	127.39
G_3	0.5	150.00	1625.13	l_{g3}	G_2	G_4	123.01
G_4	0.5	95.04	1029.68	l_{g4}	G_2	G_5	119.35
G_5	0.5	105.96	1148.09	l_{g5}	G_3	G_4	28.43
G_6	0.5	42.76	463.27	l_{g6}	G_4	G_5	25.41
G_7	0.5	12.94	140.18	l_{g7}	G_3	G_6	45.81
				l_{g8}	G_5	G_7	13.94

热力节点水质量流率与功率			热力供水管道水质量流率			
节点	水流率/(kg/s)	功率/kW	管道	起点	终点	水流率/(kg/s)
H_1	1.79	359.76	l_{s1}	H_1	H_3	0.26
H_2	1.27	255.27	l_{s2}	H_1	H_4	1.43
H_3	0.65	130.60	l_{s3}	H_5	H_4	1.16
H_4	1.56	313.55	l_{s4}	H_5	H_3	0.18
H_5	0.95	190.88	l_{s5}	H_2	H_5	1.33