

工业网络控制系统协同安全性能优化

王海凤, 黄文君, 何之栋

(浙江大学 工业控制技术国家重点实验室, 智能系统与控制研究所 杭州 310027)

E-mail: wanghaifeng422@126.com

摘要: 研究了在节点安全互相关特性及服务要求下, 工业网络控制系统中网络节点安全性能部署优化问题. 由网络化节点安全性能互相关的理论, 引入协同安全系数表征节点安全性能, 同时分析网络节点安全措施及计算性能对系统实时性的影响, 以最小化网络部署总成本为目标, 建立优化问题. 进而采用凸规划理论将对偶问题分解为安全配置与性能配置分布式问题并使用次梯度方法求解. 数值仿真结果验证了节点的互相关特性、以及安全性和实时性的制约关系, 并表明该模型可以获得收敛的优化解, 对工业控制网络设计与部署有指导意义.

关键词: 协同安全; 安全互相关; 网络部署优化; 工业网络控制系统

中图分类号: TP393

文献标识码: A

文章编号: 1000-1220(2014)09-2172-05

Optimization of Interdependent Security in Industrial Networked Control System

WANG Hai-feng, HUANG Wen-jun, HE Zhi-dong

(National Laboratory of Industrial Control Technology, Institute of Cyber-System and Control, Zhejiang University, Hangzhou 310027, China)

Abstract: Optimization of network deployment in industrial networked control system subjected to interdependent security and QoS requirements is researched. The term “Coordinated Security” is introduced on the basis of the interdependence between networked nodes facing diverse security threats. Security model and delay model are developed for each individual node. An optimization problem subjected to security and delay constraints is formulated in which the objective is to minimize network deployment cost and sub-gradient algorithm is applied to solve the problem. A case illustration is provided to demonstrate the efficiency of the proposed model, thus it is helpful for the design of industrial control network.

Key words: coordinated security; interdependent security; network deployment optimization; industrial networked control system

1 引言

工业控制网络用于连接工业控制系统中的设备节点, 负责传输采集、命令、诊断和协调等信号. 新一代的工业控制网络, 能实现工业控制网络与企业信息网络的无缝连接, 具有低成本、通用性和高扩展性等特点, 广泛应用于工业自动化和控制领域.^[1]

然而, 工业控制网络在享受开放互联技术带来的进步与效率的同时, 也开始面临越来越严重的安全威胁.^[2] 首先, 控制系统中采用了许多商用 IT 设备, 易遭受相关的软件和硬件失效. 其次, 工业网络中的通信协议日益开放, 为攻击者提供了一定的便利条件. 此外, 远程用户可以通过企业信息网获取现场的传感器和控制器数据, 使系统面临内部攻击者的攻击. 因此, 工业控制网络的安全问题已引起了很多关注.

随着攻击技术的多样化和复杂化, 如果仅仅针对每个物理点来部署检测及防御措施, 会造成资源的极大浪费, 而可以利用通信网络的特性去建立安全技术的协同作用. 文献[4]首次提出了互相关安全模型, 用以描述在复杂环境中系统之间的安全存在相互依赖关系. 需要加强本段描述文献[5]在此基础上, 针对关键基础设施从系统层面研究工业控制系统

的安全互相关性. 结果表明系统之间的安全策略选择是一个博弈问题. 但是文献[4, 5]仅以系统为研究对象研究了协同安全的共同作用, 而本文则将利用协同安全作用表征节点之间安全性相互影响的关系, 进一步以网络节点个体为目标优化系统安全特性.

有别于传统网络, 工业控制网络是连接工业现场测量控制设备的一类特殊通信网络. 它不但要完成非实时信息的通信, 而且还要求支持实时信息的通信. 因此, 在网络部署时需要估算传输时延使其满足一定的实时性要求. 实时性是工业控制系统中重要服务质量之一. 对于实时性的模型及评估, 文献[6]估计了网络中全部为周期数据流时, 在交换机内的排队概率及相应的排队时延方法. 文献[7]等针对交换式工业控制网络运用网络演算理论计算周期性和突发性实时数据的最大网络时延.

本文以工业控制网络为背景, 研究网络节点的部署问题, 主要考虑节点的安全配置和性能配置. 在网络节点(如交换机等)中设置安全互相关的影响关系引入协同安全系数建立协同安全模型; 同时考察节点安全等级对传输性能的影响, 进而基于排队论建立网络时延模型. 综合网络对实时性及安全性需求以最小化部署总成本为目标, 建立优化问题, 并采用次

收稿日期: 2012-03-26 收修改稿日期: 2013-09-01 基金项目: 国家“八六三”高技术研究发展计划项目(2012AA041105)资助. 作者简介: 王海凤, 女, 1990年生, 硕士研究生, 研究方向为安全网络控制系统; 黄文君(通信作者), 男, 1972年生, 硕士, 高级工程师, 研究方向为自动控制技术、实时分布式控制系统、工业以太网技术的研究与开发; 何之栋, 男, 1989年生, 硕士研究生, 研究方向为分布式系统、工业控制网络.

梯度算法结合分解方法进行分布式求解,结果表明利用该模型可以获得收敛的优化解,可以作为工业控制网络设计与部署的基础。

2 问题描述

本节描述工业控制网络节点性能与安全部署优化问题。优化目标是为网络中的所有节点 i 分配合适的计算性能等级 S_i 和安全性能等级 R_i , 从而完成网络的节点部署。

环网结构是工业行业中应用最广泛的一种网络结构,其特点是将中心节点和各下层节点串接成环形,在节约投资的基础上,使网络系统具有了最基本的链路冗余功能^[11]。现场设备与相连的下层节点周期性交换数据,并向中心节点汇聚。本文将以工业以太网为研究对象(如图1所示),描述优化问题及其求解。

一个节点的部署成本由计算性能等级和信息安全等级两部分引起,并作为优化问题的目标函数。优化问题的约束包括保证系统运行的时间时延、节点抵御攻击的信息安全要求和可部署的等级范围。

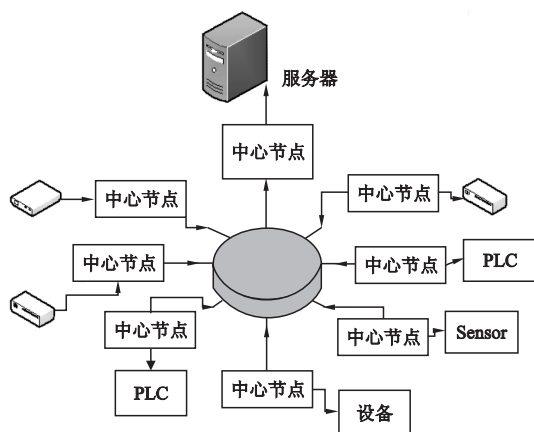


图1 环形网络结构图

Fig. 1 Network structure of ring-network

2.1 安全协同模型

为量化网络节点的安全性能,本文引入节点安全系数 γ_i 来量化节点单点安全性,

$$\gamma_i = \frac{S_i}{p_i} \quad (1)$$

其中 S_i 表示节点本身的能够影响安全的因素,用于表明自身所配置的安全措施等级 p_i 表示影响节点的安全的外部因素,用于表明节点受到的安全威胁等级。

具体地,安全措施等级是指节点的信息安全5个属性,即不可否认性、可用性、可靠性、完整性和保密性。 S_i 使用等级分值1~5表示,在对节点的安全措施等级评定时,需要结合节点的功能、所处环境和通信过程中的验证过程等进行多方面的考虑。在评定节点的安全威胁等级 p_i 时,需要分析节点所受的三种威胁,即环境威胁、暴露威胁和攻击威胁。环境威胁是指对手占有资源的丰富程度和风险程度,在工业控制网络中,体现为受攻击的概率程度。暴露威胁是节点中安全相关信息的暴露程度,如加密算法流程、用户口令设置等。攻击威胁

指攻击的深入程度和对被攻击资源的控制程度。 p_i 用0~1表示。因此,由公式(1)得出的安全系数 γ_i 越大,代表其节点的安全性能越好。

在节点相互独立时,采用上式可以准确刻画节点的安全性能,但在实际网络化模型下,需要作出一定的修改。文献[12]描述了在控制网络中,通信链路由于受网络非安全性影响,其安全性与两方面因素有关,一是自身的通信安全措施,二是在网络化连接的环境下由其他节点提供的协同检测和防御功能。本文引入了协同安全的概念,用于表征节点间的安全互相关性。网络节点的安全性不仅与其自身的节点安全系数有关,还与处于同一网络中的其他节点的安全措施等级相关。在安全互相关机制下,将式(1)扩展为协同安全系数 γ_i ,用以表征网络节点在使用共同通信介质环境下,受其他节点的安全措施影响后的实际安全性能指标,定义如下:

$$\gamma_i = \frac{S_i}{P_i + \sum_{k \in N, k \neq i} (-g_{ik}) S_k} \quad (2)$$

其中 N 为下层节点的集合, $g_{ij} \in G$ 为协同安全矩阵,用于量化节点间的互相关性。由式(2),节点协同安全系数由三者决定,自身配置的安全措施等级、节点安全威胁等级和其他节点的安全措施等级。在部署网络时,可以通过增加自身的安全措施等级和降低安全威胁等级提升协同安全系数,还可以通过增加其他节点的安全措施等级达到协同促进节点安全性的作用。

在工业通信网络中,节点之间存在直接的物理连接或连贯的数据通信关系,由此可以简单而不失一般性的设定:节点之间的安全性的依赖关系主要取决于数据通信流线路的物理传输距离,即一个节点在受到攻击时,该数据流中距离越近的节点同样有能力检测出安全威胁且检测概率越大,且呈现非线性增长关系,距离过远则影响可近似为零。因此,对于式(2)中的协同安全矩阵 $G \in \mathbb{R}^{n \times n}$,对于任意 $g_{ij} \in G$ 定义:

$$g_{ij} = \begin{cases} K & \text{if } d_{ij} \in D_{dir} \\ \frac{K}{(1 + d_{ij})^2} & \text{if } d_{ij} \in D_{indir} \\ 0 & \text{if } d_{ij} \in D_{noneffect} \end{cases} \quad (3)$$

其中 d_{ij} 表示节点 i 到节点 j 的距离, K 为基准值, D_{dir} , D_{indir} , $D_{noneffect}$ 分别为直接影响范围集、间接影响范围集和无影响范围集,直接影响范围集包括与节点直接物理连接的节点,间接影响范围集包括一定距离内与节点连接的节点,无影响范围集则是超过一定距离后安全互相关影响可忽略的节点。

2.2 时延评估模型

一个数据包从源设备发出,经过网络节点转发直至到达中心节点的时间称为传输时延,记为 D_i 。数据包的传输时延由物理路径传输时延和节点转发时延组成。

假设两个节点之间的连线长度小于10m,由于数据帧在物理链路上的传播速度为 $2 \times 10^8 \text{ m/s}$ ^[9]。考虑到当前大部分实时以太网(RTE)是基于快速以太网(Rate = 100Mbps),因此数据帧在链路上传播时延小于50ns,在数量级上很小,因此可以忽略物理路径传播时延。

由文献[8]中对以太网网络时延的分析,节点转发时延主要由数据产生节点和数据转发节点处的时延组成,在产生

节点处的时延与数据帧长度 L_i 和节点服务速率 v_i 相关,在转发节点处的时延与该点处的平均队列和节点服务速率相关.由前面的分析,节点服务速率 v_i 与节点性能等级 R_i 呈正相关.由此,定义节点 i 处的数据包传输时延 D_i :

$$D_i = \alpha \frac{(1 + S_i)}{(R_i + 1)} + \sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} \quad (4)$$

式中,前一项表示数据在本节点的处理时间,由于安全措施如加密等会在数据帧中增加一定的附加位,简单不失一般性地,设定数据帧长度与安全等级 s_i 成线性关系,而处理速度与节点计算性能成正比.第二项表示由排队效应引起的转发时延,其主要因素包括转发节点处的队列长度及转发性能^[8,9],其中 Q_{avg} 表示在转发节点处的平均队列长度,转发时间与平均队列长度成正比. α 和 β 为权重因子, N_i 为固定网络拓扑下节点 i 到中心节点路径上所经过的节点集合.

2.3 优化问题描述

工业以太环网的部署过程中,随网络节点安全性能等级以及计算性能等级的不同,其配置的成本也不同,且等级越高,成本的上升越快.因此,定义网络中节点的成本为 C_i ,由部分组成,分别是性能配置成本以及安全配置成本:

$$C_i = C_{i,sec} + C_{i,perf} = \sum_{i \in N} \lambda U_s(S_i) + \sum_{i \in N} U_R(R_i) \quad (5)$$

为了给网络中的所有节点分配合适的安全等级和性能等级,建立优化问题模型.优化的目标为最小化配置成本,需要满足的约束包括两方面,既要满足一定的安全等级,又要使得部署的网络能够符合工业环境下对实时性的要求.综上所述,目标优化问题如下:

$$\min \sum_{i \in N} \lambda U_s(S_i) + \sum_{i \in N} U_R(R_i) \quad (6-a)$$

$$s. t. D_i \leq T_i^d \quad \forall i \in N \quad (6-b)$$

$$\gamma_i \geq \gamma_i^{\min} \quad \forall i \in N \quad (6-c)$$

$$S_{\min} \leq S_i \leq S_{\max} \quad \forall i \in N \quad (6-d)$$

$$R_{\min} \leq R_i \leq R_{\max} \quad \forall i \in N \quad (6-e)$$

其中,式(6a)表示时延约束, D_i 表示节点 i 处的数据包传输时延, T_i^d 为时延上界,式(6b)表示安全性能约束, γ_i 为节点 i 的安全系数, γ_i^{\min} 为安全性能等级的下界,式(6c)和式(6d)表示自变量约束, S_{\min} (S_{\max}) 和 R_{\min} (R_{\max}) 分别为安全措施等级和计算性能等级的下界(上界).

3 问题求解

由于目标函数为严格的凸函数,约束条件为线性函数,上述优化问题是严格的凸规划问题.分别为约束集(6-a)至(6-d)引入对偶变量 $\bar{\omega}_i, \mu_i, \varphi_i, \psi_i, \forall i \in N$, 释放部分约束条件,则式(6)中的优化问题可以转化为公式 Lagrange 形式,见式(7).

$$L = \left\{ \sum_{i \in N} \lambda U_s(S_i) + \sum_{i \in N} U_R(R_i) + \sum_{i=1}^N \bar{\omega}_i \left(\alpha(1 + S_i) + (R_i + 1) \left(\sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} - T_i^d \right) \right) + \sum_{i=1}^N \mu_i \left(\gamma_i^{\min} p_i - \left(S_i + \sum_{k \in N_i} \gamma_i^{\min} g_{ik} S_k \right) \right) + \sum_{i=1}^N \varphi_i (S_i - S_{\max}) + \sum_{i=1}^N \psi_i (R_i - R_{\max}) \mid S_{\min} \leq S_i, R_{\min} \leq R_i \right\} \quad (7)$$

重新排列式(7)后,分离变量可将问题分为安全分配和性能分配子问题,则优化问题可用式(8)描述:

$$L = \left\{ \sum_{i \in N} \lambda U_s(S_i) + \sum_{i=1}^N \bar{\omega}_i \alpha (1 + S_i) + \sum_{i=1}^N \mu_i \left(\gamma_i^{\min} p_i - \left(S_i + \sum_{k \in N_i} \gamma_i^{\min} g_{ik} S_k \right) \right) + \sum_{i=1}^N \varphi_i (S_i - S_{\max}) \mid S_{\min} \leq S_i \right\} + \left\{ \sum_{i \in N} U_R(R_i) + \sum_{i=1}^N \bar{\omega}_i (R_i + 1) \left(\sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} - T_i^d \right) + \sum_{i=1}^N \psi_i (R_i - R_{\max}) \mid R_{\min} \leq R_i \right\} \quad (8)$$

3.1 子问题求解

在转化为对偶问题后可将式(8)的问题分解为安全性能分配子问题和计算性能分配子问题,并采用分布式算法求解.

1) 安全性能分配问题

$$\min L_s = \sum_{i \in N} \left\{ \lambda_i U_s(S_i) + \bar{\omega}_i \alpha (1 + S_i) + \mu_i \left(\gamma_i^{\min} p_i - \left(S_i + \sum_{k \in N_i} \gamma_i^{\min} g_{ik} S_k \right) \right) + \varphi_i (S_i - S_{\max}) \right\} \quad (9)$$

$$s. t. S_{\min} \leq S_i \quad \forall i \in N$$

设定 $U_i(S_i) = \log(S_i)$, 根据 KKT 条件^[13], 使 $\frac{\partial L_s}{\partial S_i} = 0$, 上述问题的解为:

$$S_i = \max \left\{ S_{\min}, \frac{\lambda_i}{\mu_i - \bar{\omega}_i \alpha - \varphi_i} \right\} \quad (10)$$

2) 计算性能分配问题

$$\min L_p = \sum_{i \in N} \left\{ U_R(R_i) + \bar{\omega}_i (R_i + 1) \left(\sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} - T_i^d \right) + \psi_i (R_i - R_{\max}) \right\} \quad (11)$$

$$s. t. R_{\min} \leq R_i \quad \forall i \in N$$

设定 $U_i(R_i) = R_i^2$, 根据 KKT 条件可得该问题的解:

$$R_i = \max \left\{ R_{\min}, \left(\bar{\omega}_i \left(T_i^d - \sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} \right) - \psi_i \right) / 2\lambda \right\} \quad (12)$$

3.2 对偶问题

原始优化问题的对偶形式^[14]如下:

$$\max g(\bar{\omega}, \mu, \varphi, \psi)$$

$$s. t. \bar{\omega}, \mu, \varphi, \psi > 0$$

其中 $g(\bar{\omega}, \mu, \varphi, \psi) = L(S^*, R^*, \bar{\omega}, \mu, \varphi, \psi)$. 对偶变量 $\bar{\omega}_i, \mu_i, \varphi_i, \psi_i$ 的更新可通过分别对 $g(\bar{\omega}, \mu, \varphi, \psi)$ 求对应变量的偏导数获得. 对偶变量的更新规则如下:

$$\bar{\omega}_i(k+1) = \max \left\{ 0, \bar{\omega}_i(k) + \beta_{\omega} \left(\alpha(1 + S_i) + (R_i + 1) \left(\sum_{k \in N_i} \beta \frac{Q_{avg}}{(R_k + 1)} - T_i^d \right) \right) \right\} \quad (13-a)$$

$$\mu_i(k+1) = \max \left\{ 0, \mu_i(k) + \beta_{\mu} \left(\gamma_i^{\min} p_i - \left(S_i + \sum_{k \in N_i} \gamma_i^{\min} g_{ik} S_k \right) \right) \right\} \quad (13-b)$$

$$\varphi_i(k+1) = \max \{ 0, \varphi_i(k) + \beta_{\varphi} (S_i - S_{\max}) \}, \forall i \in N \quad (13-c)$$

$$\psi_i(k+1) = \max\{0, \mu_i(k) + \beta_\psi(R_i - R_{\max})\}, \forall i \in N \quad (13-d)$$

其中 $\beta_\omega, \beta_\mu, \beta_\varphi, \beta_\psi$ 为非负的迭代步长。

3.3 算法步骤

- 1) 对于网络中的每个节点, 给定初始性能等级 $R_i(0)$ 和初始安全等级 $S_i(0)$;
- 2) 对于给定的 $\bar{\omega}_i(t), \mu_i(t), \varphi_i(t), \psi_i(t)$ 按照式(10)、式(12)迭代更新安全等级 S_i 和性能等级 R_i ;
- 3) 按式(13-a)至式(13-d)更新 Lagrange 因子 $\bar{\omega}_i(t+1), \mu_i(t+1), \varphi_i(t+1), \psi_i(t+1)$;
- 4) 返回步骤2直至算法收敛。

4 仿真方案与结果分析

为评估次梯度法与分解方法在工业控制网络的部署问题求解中的性能表现, 以下将针对给定的网络进行模拟与仿真, 以进一步分析与验证网络部署中安全等级与性能等级提升的关系。

如图2所示, 本文采用环网拓扑进行测试, 测试拓扑共设有10个节点, 节点间通信为有线通信, 其中Y1为中心节点, N1~N9为下层节点, 下层节点分别接有一个现场设备, 在一个周期内, 每个节点从现场设备处接收一包数据帧并转发至中心节点。数据帧在物理链路上的传播速度为 2×10^8 m/s, 节点周期性发送数据包至中心节点, 每秒10帧数据包。公式(4)中的权重因子 α 和 β 均设为0.5。



图2 测试拓扑图

Fig. 2 Topology for numerical testing

所有节点设置相同的最低协同安全要求 $\gamma_i^{\min} = 8$, 并假设节点威胁等级 p_i 均相同, 设为0.4。对于协同安全矩阵, 由于测试拓扑为环网结构, 直接影响范围集 D_{dir} 为与节点相邻的节点, 间接影响范围集为跳数小于5以内范围的节点集合, 其余节点属于无影响范围集。由于环网中每个节点的数据都汇聚到中心节点, 距离中心节点近的节点转发量大, 故假设节点处的平均排队队列长度与该距离成线性反比。

在上述测试拓扑下, 可获得每个节点分配的安全性能等级和计算性能等级, 如图3所示。由于受其他节点的影响, 拓扑中的节点并未单纯采用安全最低限度, 其中节点5的安全性能等级最低, 这是由于其在拓扑中不作为其他节点的中继节点, 在该点处继续增加安全措施对提高整体安全性的影响很小。从计算性能等级的分配看, 安全性能等级的提高对计算性能等级有一定的影响。例如, 尽管节点2和节点3在拓扑上相近, 但节点3分配的计算性能高于节点2, 主要是由于节点3以实时性为代价而采取较高的安全等级措施。图4为目标

函数值的迭代曲线, 利用本文提出的算法可以在较短时间内使优化问题收敛, 计算速度较快。

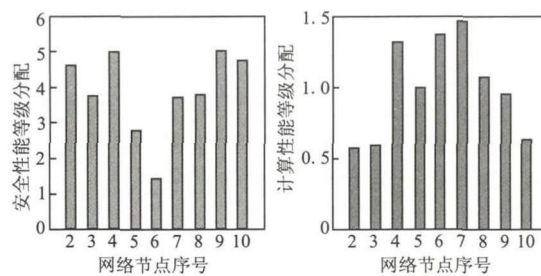


图3 节点分配安全性能 VS 节点分配计算性能

Fig. 3 Security levels deployed for nodes VS computation capacity deployed for nodes

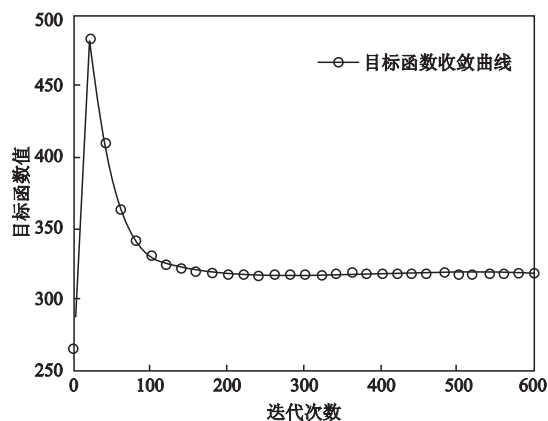


图4 目标函数值优化结果

Fig. 4 Numerical optimization result

为了进一步说明安全互相关性对环形网络的影响, 还测试了相同安全和计算性能要求下, 随着拓扑大小变化, 所有节点分配的平均性能的变化情况。由图5可以看出, 随着网络节

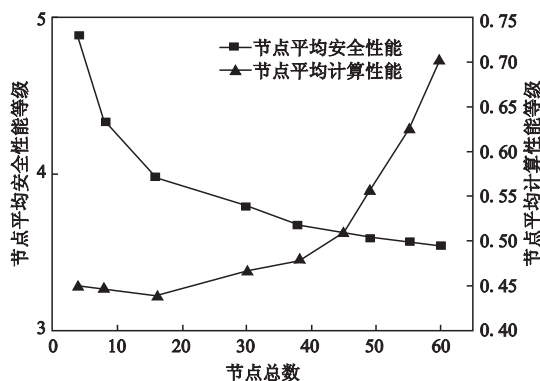


图5 不同网络规模下的性能分配对比

Fig. 5 Security versus computation capacity deployment within different network scales

点的增加, 节点分配的平均安全性能等级降低且趋于平缓, 而分配的平均计算性能等级增加。这是由于在环网结构下, 节点之间相互连接, 随着网络规模的增大, 节点受益于安全互相关性, 在安全要求相同的情况下, 只需要采取较低的安全等级措施即可满足条件, 但当规模增大到一定程度后, 增加节点产生

的协同影响很小,环网中的节点趋于平衡态,节点平均安全等级措施不再有明显的下降趋势。此外,由于节点增加负载增大,对实时性造成一定影响,因此节点需要更高的计算性能。

5 结 语

本文基于安全互相关模型建立网络控制系统部署配置优化问题,并采用次梯度分布式算法求解,获得特定网络拓扑下的节点性能配置方案。数值仿真验证了节点的互相关特性、以及安全性和实时性的制约关系。通过该模型可以获得收敛的优化解,可以同时满足工业网络控制系统对于实时性和安全性的高要求。本文建立的模型可以作为工业控制网络设计与部署的基础,辅助工程师进行控制系统的设计。

本文在仿真过程中,仅对环网结构进行了仿真与分析,在今后的工作中,将对其他常用的工业网络结构,如星形拓扑结构和总线型结构等进行分析,以达到更符合工业环境的效果。同时,在系统安全等级的量化中,目前采用等级制,今后考虑在对节点进行工艺分析的基础上,研究相应的量化模型。

References:

- [1] Huang Wen-jun, Xie Dong-kai, Lu Shan, et al. Design of high availability redundancy industrial ethernet[J]. Chinese Journal of Scientific Instrument 2010, 33(3): 704-708.
- [2] Stouffer, Keith, Joe Falco, Karen Scarfone. Guide to industrial control systems(ICS) security[S]. NIST Special Publication, 2008, 800-82.
- [3] Zhang You-dong, Zeng Qing-kai, Wang Jian-dong. Studies of network coordinative forensics computing[J]. Chinese Journal of Computers 2010, 33(3): 504-512.
- [4] Kunreuther H, Heal G. Interdependent security[J]. Journal of Risk and Uncertainty 2003, 26(2): 231-249.
- [5] Amin, Saurabh, Schwartz G A, Sastry S S. Security of interdependent and identical networked control systems. ser[Z]. TRUST Working Papers, Berkeley, CA(2010).
- [6] Cupek, Rafał, Łukasz Huczala. Field level industrial ethernet network data analysis[J]. Computer Networks 2011: 358-366.
- [7] Zhang Lei, Zhi Wang. Real-time performance evaluation in hybrid industrial ethernet networks[C]. World Congress on Intelligent Control and Automation ((WCICA), 2010 8th World Congress on. IEEE 2010.
- [8] Li Shao-wu. Research on real-time performance of network control system based on industrial ethernet[D]. Shenyang: Northeast University 2008.
- [9] Hu Guo-chuan. End-to-end delay modeling and performance analysis of industrial ethernet[D]. Jiangsu: Zhejiang University 2012.
- [10] Kumar V S, et al. Existence theorems and approximation algorithms for generalized network security games[C]. Distributed Computing Systems(ICDCS), 2010 IEEE 30th International Conference on. IEEE 2010.
- [11] Zhang Yu-hui. The research of the control system based on the industrial ethernet ring network[D]. Guang Southern Technical University 2012.
- [12] Hare Forrest, Jonathan Goldstein. The interdependent security problem in the defense industrial base: an agent-based model on a social network[J]. International Journal of Critical Infrastructure Protection 2010, 31(3): 128-139.
- [13] Boyd S, Gallager R G. Data networks[M]. Englewood Cliffs, NJ: Prentice-Hall, 1991.
- [14] Palomar D P, Chiang M. A tutorial on decomposition methods for network utility maximization[J]. IEEE J. Sel. Areas Commun., 2006, 24(8): 1439-1451.
- [15] Ren Qing-zhen, Zhang Jun, Huang Tian-wu. Study of fieldbus control system and the analysis of its real-time character[J]. Measurement & Control Technology 2004, 23(4): 37-40.
- [16] Fan Gao-xian, Zhou Bo, Ying Qing-ping. Application of industrial ethernet ring network in mine safe surveillance systems[J]. Industry and Mine Automation 2007, 12(6): 108-110.
- [17] Vaughn, Rayford B, Thomas Morris, et al. Development & expansion of an industrial control system security laboratory and an international research collaboration[C]. Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, ACM 2013.
- [18] Zhou Huan-sheng, Jiang Jian-hui. A multi-dimensional security index system and quantitative level protection model[J]. Journal of University of Science and Technology of China 2012, 42(1): 67-76.

附中文参考文献:

- [1] 黄文君, 谢东凯, 卢山, 等. 一种高可用性的冗余工业实时以太网设计[J]. 仪器仪表学报 2010, 33(3): 704-708.
- [3] 张有东, 曾庆凯, 王建东. 网络协同取证计算研究[J]. 计算机学报 2010, 33(3): 504-512.
- [8] 李绍武. 基于工业以太网的网络控制系统实时性研究[D]. 沈阳: 东北大学 2008.
- [9] 胡国传. 工业以太网端到端时延的建模与分析[D]. 江苏: 浙江大学 2012.
- [11] 张宇辉. 基于工业以太环网的控制系统关键技术研究[D]. 广州: 华南理工大学 2012.
- [15] 任清珍, 张军, 黄天戌, 等. 现场总线控制系统的进步性及其实时性研究[J]. 测控技术 2004, 23(4): 37-40.
- [16] 范高贤, 周波, 殷庆平. 光纤工业以太环网在煤矿安全监控系统中的应用[J]. 工矿自动化 2007, 12(6): 108-110.
- [18] 周焕盛, 江建慧. 一个多维信息安全指标体系及等级保护量化模型[J]. 中国科学技术大学学报 2012, 42(1): 67-76.