DOI:10.20033/j.1003-7241.(2025)12-0061-06

基于多属性决策的 SCADA 系统轻量级安全防护措施决策模型

邓正东[1]，雷宣念[1]，梁俊宇[2]，许　航[1]，朱志远[1]，李中伟[3]
（1.云南电网有限责任公司 楚雄供电局,云南 楚雄 675000；2.云南电网有限责任公司 云南电力科学研究院,云南 昆明 650000；
3.哈尔滨工业大学 电气工程及自动化学院,黑龙江 哈尔滨 150000）

摘　要:随着嵌入式系统的广泛应用,选择适当的轻量级安全防护措施以提升资源受限终端的安全水平变得尤为重要。为此,在考虑网络安全防护措施的资源消耗属性、时间延迟属性及安全收益属性的基础上,建立轻量级防护措施决策的属性目标函数,利用层次分析法确定各属性的权重,构建基于多属性决策的决策模型,根据决策值完成对备选防护措施的优选,解决了传统防护方案选择防护措施主观性强的问题。于搭建的模拟控制系统(supervisory control and data acquisition, SCADA)数据采集与监视控制系统中应用所提轻量级安全防护措施决策模型,结果表明所提模型能够有效选择轻量级安全防护措施。

关键词:SCADA 系统;轻量级防护;防护措施决策;层次分析法;多属性决策;网络安全
中图分类号: TP183　　**文献标志码**: A　　**文章编号**: 1003-7241(2025)12-0061-06

Decision model for lightweight safety protection measures in SCADA system based on multi-attribute decision-making

DENG Zhengdong[1], LEI Xuannian[1], LIANG Junyu[2], XU Hang[1], ZHU Zhiyuan[1], LI Zhongwei[3]
(1. Chuxiong Power Supply Bureau, Yunnan Power Grid Corporation Ltd., Chuxiong 675000, China;
2. Yunnan Power Grid Corporation Ltd., Yunnan Electric Power Research Institute, Kunming 650000, China;
3. Harbin Institute of Technology, School of Electrical Engineering and Automation, Harbin 150000, China)

Abstract: With the widespread application of embedded systems, it becomes increasingly important to select appropriate lightweight security measures to enhance the security levels of resource-constrained terminals. Therefore, this paper establishes an attribute objective function for the decision-making of lightweight security measures by considering the resource consumption, time delay, and security benefit attributes of network security measures. A multi-attribute decision-making model is constructed using the analytic hierarchy process (AHP) to determine the weights of each attribute, allowing for the optimal selection of alternative security measures based on decision values. This approach addresses the subjectivity issue commonly associated with traditional security measure selection. The proposed decision-making model for lightweight security measures is applied to a simulated supervisory control and data acquisition system, and the results demonstrate that the model effectively identifies suitable lightweight security measures.

Keywords: supervisory control and data acquisition (SCADA) system; lightweight protection; selection of protective measures; analytic hierarchy process; multi-attribute decision-making; network security

0　引言

随着信息技术的快速发展,SCADA 系统逐步采用网络化的通信系统与开放的通信协议,一旦该系统遭受黑客入侵,极易引发系统崩溃甚至电网大面积停电[1-3]。文献[4]将 AES 加密层置于 PLC 网络层以防止拦截、注入和 DOS 攻击。文献[5]采用基于 NTRU 的加密和认证方案解决 SCADA 系统中的数据完整性、保密性和认证问题。文献[6]结合 Modbus 和传输层安全协议实现安全通信,并比较分组密码与流密码的处理时间。文献[7]为工业 SCADA 系统设计了一种 Modbus 安全协议,测试其时间与安全性能。文献[8]在单个 FPGA 上实现轻量级加密的密码系统,提供低成本的 SCADA 安全设备。文献[9]提出远程监控安全通信方案,利用客户端认证令牌的 TLS 加密。文献[10]针对油气管道 SCADA 系统的网络攻击问题,提出分层参考模型和安全区域划分框架。文献[11]基于恶意程序识别算法构建油气 SCADA 主动防御系统。文献[12]提出基于区块链的 SRAM PUF 身份认证协议,确保数据完整性。文献[13]比较传统 SCADA 系统在虚假命令注入攻击下的检测与响应方法。文献[14]针对智能电网中缺乏可信身份认证机制的问题,提出使用光纤区块链管理加密密钥的身份认证方案。

综上所述,当前针对 SCADA 系统的网络安全研究主要集中在为整体 SCADA 系统提供完整的安全防护方案,而忽视了嵌入式终端的网络安全问题。由于嵌入式终端计算资源有限,因此如何在防护方案设计中选择最具轻量性的防护措施成为一大难点。为此,本文提出了一种多属

* 基金项目:工信部 2020 年工业互联网创新发展工程项目(TC200H01Q)
收稿日期:2024-09-23

性决策模型,考虑资源消耗、时间延迟和安全收益 3 个属性,以决策值为导向进行备选防护措施的选择。最终,于搭建的模拟 SCADA 系统验证了本文所提模型的有效性。

1 SCADA 系统网络安全防护方案

攻击者针对 SCADA 系统的攻击手段多种多样,常见的攻击手段如窃取攻击,攻击者通过监听网络,获取 SCADA 系统各层设备之间传输的信息;重放攻击,攻击者窃取到告警信息后,直接重复地将其发送给集控中心层,从而导致错误决策;篡改攻击,SCADA 系统中传输的信息遭受攻击者拦截并恶意篡改,集控中心根据篡改过的信息进行决策将产生错误的控制指令[15]。除考虑攻击行为之外,现场存在大量嵌入式终端,其计算资源有限,因此,需要权衡防护措施的安全性与轻量性。

SCADA 系统采用典型的分层体系结构,主要设备包括集控中心服务器(central control server,CCS)、就地控制服务器(local control server,LCS)和 RTU、PLC、IED 等终端设备。考虑到资源受限的嵌入式终端网络安全防护能力不足,本文设计了 SCADA 系统网络安全防护方案,具体如图 1 所示,包括各层设备间双向身份认证措施和信息加密认证措施等。通信前 RTU、LCS 与 CCS 利用数字签名和 Hash 算法进行双向身份认证。通信过程中,RTU、LCS 与 CCS 对信息进行加密和认证,因防护措施的资源需求不同,RTU 与 LCS 信息加密认证采用对称加密和 Hash 算法,LCS 与 CCS 信息加密认证采用非对称加密和数字签名。

在设备间的双向身份认证和信息加密过程中,密码算法、Hash 算法和数字签名算法是确保系统安全性的关键。目前应用广泛的非对称密码算法为基于椭圆曲线的 ECC 加密算法[16]和 SM9 加密算法,适宜在安全性要求较高的场景下使用。目前针对资源受限环境设计的 Hash 算法有 LHash-64 和 Quark 系列算法。ECDSA 算法和 SM9 数字签名算法是在嵌入式装置中应用的较为轻量的数字签名算法。因此,选择适当的轻量级网络安全防护措施对于在有限资源环境下确保嵌入式装置的轻量性与安全性至关重要。

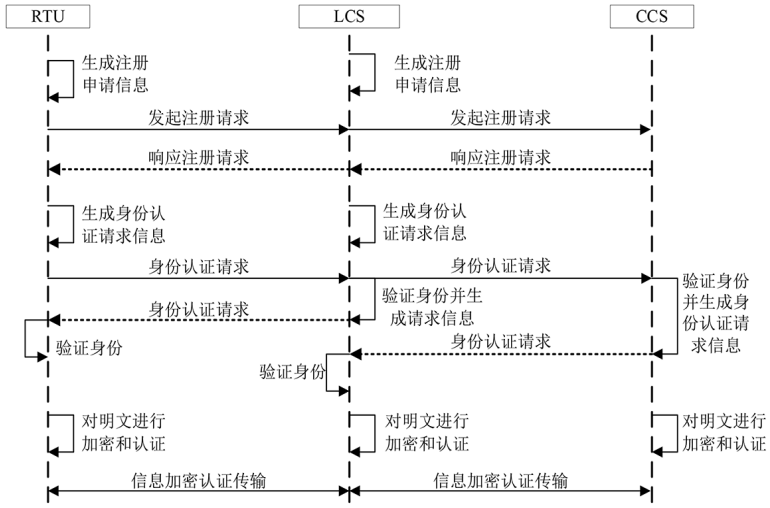

图 1 SCADA 系统网络安全防护方案

2 轻量级网络安全防护措施决策模型建立

在 SCADA 系统中,嵌入式终端面临计算资源有限、实时性要求高和安全性保障的多重挑战。现有的轻量级密码算法种类较多,不同长度的密钥设定也将影响算法的轻量性和安全性。因此,为了在保障安全性的同时最大限度地减少系统资源消耗和响应延迟,需要对不同的防护措施进行有效选择。本文建立多属性决策模型,结合风电场 SCADA 系统的计算资源约束和实时性要求,从资源消耗、时间延迟和安全收益三个角度权衡网络安全防护措施的选择。此模型旨在为 SCADA 系统中的嵌入式终端提供一个量化、系统化的决策框架,帮助选择最合适的轻量级网络安全防护措施。这一模型的建立,有助于平衡系统性能与安全需求,在满足轻量性要求的同时,确保网络防护的有效性和高效性。

2.1 属性目标函数建立

2.1.1 资源消耗属性

本文选定的资源消耗属性包括 CPU 利用率 P_C、堆栈利用率 P_S 和内存占用空间 P_M。计算备选措施的资源消耗,需要权衡各组成要素对设备的重要程度并确定各组成要素的权重。为统一各组成要素的量纲,便于决策矩阵的计算,利用式(1)最值归一化方法对 P_C、P_S 和 P_M 进行归一化处理。资源消耗属性各组成要素归一化处理后结果为 P_C'、P_S' 和 P_M'。

$$P_{\text{normalization}} = \frac{P_i - P_{\min}}{P_{\max} - P_{\min}} \tag{1}$$

式中,$P_{\text{normalization}}$ 为资源消耗属性的组成要素进行最值归一化的结果,P_i 为组成要素,$P_{\min}$ 为组成要素的最小值,$P_{\max}$

为组成要素的最大值。

则资源消耗目标函数如式(2)所示。

$$\mathrm{CON} = w_{\mathrm{C}}P_{\mathrm{C}}^{'} + w_{\mathrm{S}}P_{\mathrm{S}}^{'} + w_{\mathrm{M}}P_{\mathrm{M}}^{'} \tag{2}$$

式中,CON 为备选措施资源消耗值; w_{C}、w_{S}、w_{M} 分别为 $P_{\mathrm{C}}^{'}$、$P_{\mathrm{S}}^{'}$ 和 $P_{\mathrm{M}}^{'}$ 的权重,且 $w_{\mathrm{C}} + w_{\mathrm{S}} + w_{\mathrm{M}} = 1$。

2.1.2 时间延迟属性

本文以 P_{T} 表示备选措施的处理时间,由于光纤通信的传输时间较短可以忽略不计,因此时间延迟只考虑密码算法的计算、处理时间,时间延迟目标函数如式(3)所示。

$$\mathrm{DEL} = P_{\mathrm{T}} \tag{3}$$

式中,DEL 为备选措施时间延迟值。

2.1.3 安全收益属性

在安全收益的组成要素中,包括信息完整性 P_{I}、信息机密性 P_{P} 和信息不可否认性 P_{N}。

P_{I} 取决于所选 Hash 算法的安全性能,而评判 Hash 算法的安全性能可以从抗碰撞性的角度去计算。本文将 Hash 算法的抗碰撞性映射到[0,1]区间,将映射值作为 P_{I} 量化指标。其中 N 为 Hash 算法输出的消息摘要值长度位数,则该 Hash 算法的抗碰撞性为 $N/2$。

$$P_{\mathrm{I}} = f\left(\frac{N}{2}\right) = \frac{\log_2\frac{N}{2} - \log_2\frac{N_{\min}}{2}}{\log_2\frac{N_{\max}}{2} - \log_2\frac{N_{\min}}{2}} \tag{4}$$

P_{P} 取决于加密算法的安全强度,本文利用线性转换公式将密码算法的密钥长度 L_{key} 映射到[0,1]区间,将映射值作为 P_{P} 量化指标。

为保障通信双方不可否认发送和接收的信息,使用数字签名对信息进行验证。本文对 P_{N} 选择以数字签名的私钥长度 L_{private} 来衡量,并利用线性转换公式将数字签名的私钥长度映射到[0,1]区间,将映射值作为 P_{N} 的量化指标。

根据 P_{I}、P_{P} 和 P_{N} 构建的安全收益目标函数如式(5)所示。

$$\mathrm{INC} = w_{\mathrm{I}}P_{\mathrm{I}} + w_{\mathrm{P}}P_{\mathrm{P}} + w_{\mathrm{N}}P_{\mathrm{N}} \tag{5}$$

式中,INC 表示安全防护措施的安全收益值;w_{I}、w_{P} 和 w_{N} 表示信息完整性、信息机密性和信息不可否认性的权重,且 $w_{\mathrm{I}} + w_{\mathrm{P}} + w_{\mathrm{N}} = 1$。

2.2 基于层次分析法的目标函数权重赋值

层次分析法(analytic hierarchy process, AHP)是一种多准则决策分析方法,旨在帮助决策者在复杂问题下作出最佳决策,特别是涉及多个标准或因素的决策。因此,在计算前文建立的目标函数时,选用层次分析法确定各属性目标函数中各指标的权重。

构建如式(6)所示的判断矩阵 $\boldsymbol{A}$,用来表示要素之间的重要度,矩阵中元素 $a_{i,j}$ 代表第 i 个元素比第 j 个元素的重要程度,$a_{i,j}$ 与 $a_{j,i}$ 互为倒数。

$$\boldsymbol{A} = (a_{i,j})_{n\times n} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix} \tag{6}$$

重要程度共划分成 9 个等级,判断矩阵 $\boldsymbol{A}$ 中元素的取值为 1~9,具体元素重要度如表 1 所示。

表 1 元素重要度

a_{ij}	第 i 个指标相对第 j 个指标重要度
1	同等重要
2	介于>1~3 之间
3	稍微重要
4	介于>3~5 之间
5	比较重要
6	介于>5~7 之间
7	强烈重要
8	介于>7~9 之间
9	极端重要

由于判断矩阵 $\boldsymbol{A}$ 中的元素为主观设定,需要验证判断矩阵的合理性。因此,在计算权重之前,利用公式(7)计算一致性 CR,一致性检验合格需要满足 $\mathrm{CR} < 0.1$。

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{7}$$

式中,RI 为随机性一致指标;CI 为一致性校验指标。

在进行资源消耗和安全收益的指标权重计算时,判断矩阵均为 3 阶,通过查阅随机一致性指标表获得 RI 值为 0.52,通过式(8)求得 CI。

$$\mathrm{CI} = \frac{\lambda_{\max} - n}{n - 1} \tag{8}$$

式中,$\lambda_{\max}$ 为判断矩阵的最大特征值;n 为判断矩阵的阶数。

一致性检验通过后,利用算数平均值对判断矩阵计算权重 w_I 如式(9)所示。

$$w_I = \frac{1}{n}\sum_{j=1}^{n}\frac{a_{ij}}{\sum_{k=1}^{n}a_{kj}},\ i = 1,2,\cdots,n \tag{9}$$

2.2.1 资源消耗目标函数权重

本文参考文献[16]中内存占用空间、算法复杂度等指标的相对重要程度构建了资源消耗组成元素判断矩阵,以表示资源消耗中 CPU 利用率、堆栈利用率和内存占用空间的相互重要程度,并进行一致性检验,计算结果如表 2 所示。利用 AHP 计算出 $w_{\mathrm{C}} = 0.676\ 8$、$w_{\mathrm{S}} = 0.130\ 7$、$w_{\mathrm{M}} = 0.192\ 5$。则资源消耗的目标函数如式(10)所示。

$$\mathrm{CON} = 0.676\ 8P_{\mathrm{C}} + 0.130\ 7P_{\mathrm{S}} + 0.192\ 5P_{\mathrm{M}} \tag{10}$$

2.2.2 安全收益目标函数权重

本文参考文献[17]中信息完整率、信息准确率等指标的相对重要程度为参考构建安全收益判断矩阵。利用 AHP,计算出 $w_{\mathrm{I}} = 0.698\ 5$、$w_{\mathrm{P}} = 0.090\ 1$ 和 $w_{\mathrm{N}} = 0.211\ 5$。安全收益的目标函数如式(11)所示。

$$\mathrm{INC} = 0.698\ 5P_{\mathrm{I}} + 0.090\ 1P_{\mathrm{P}} + 0.211\ 5P_{\mathrm{N}} \tag{11}$$

表 2　资源消耗目标函数权重计算结果

判断矩阵	一致性校验	特征值	权重向量
$\begin{bmatrix} 1 & 4 & 5 \\ 1/4 & 1 & 1/2 \\ 1/5 & 2 & 1 \end{bmatrix}$	CR = 0.090 3 < 0.1	$\lambda_1 = 3.094$ $\lambda_2 = -0.047 + 0.537\,3\mathrm{j}$ $\lambda_3 = -0.047 + 0.537\,3\mathrm{j}$ $\lambda_{max} = 3.094$	$\begin{bmatrix} 0.676\,8 \\ 0.130\,7 \\ 0.192\,5 \end{bmatrix}^{T}$

表 3　安全收益目标函数权重计算结果

判断矩阵	一致性校验	特征值	权重向量
$\begin{bmatrix} 1 & 6 & 5 \\ 1/6 & 1 & 1/3 \\ 1/5 & 3 & 1 \end{bmatrix}$	CR = 0.077 3 < 0.1	$\lambda_1 = 3.154\,6$ $\lambda_2 = -0.077\,3 + 0.481\,4\mathrm{j}$ $\lambda_3 = -0.077\,3 + 0.481\,4\mathrm{j}$ $\lambda_{max} = 3.154$	$\begin{bmatrix} 0.698\,5 \\ 0.090\,1 \\ 0.211\,5 \end{bmatrix}^{T}$

2.3　资源-时间-安全多属性决策模型

根据前文确定的属性目标函数，本文确定 SCADA 系统轻量级网络安全防护措施决策函数，并根据决策函数建立决策矩阵为

$$\begin{cases} \min \mathrm{CON} = 0.676\,8 \cdot P_{\mathrm{C}} + 0.130\,7P_{\mathrm{S}} + 0.192\,5P_{\mathrm{M}} \\ \min \mathrm{DEL} = P_{\mathrm{T}} \\ \max \mathrm{INC} = 0.698\,5 \cdot P_{\mathrm{I}} + 0.090\,1 \cdot P_{\mathrm{P}} + 0.211\,5 \cdot P_{\mathrm{N}} \end{cases} \tag{12}$$

$$\boldsymbol{DM} = \begin{bmatrix} ar_{11} & ar_{12} & ar_{13} \\ ar_{21} & ar_{22} & ar_{23} \\ \vdots & \vdots & \vdots \\ ar_{m1} & ar_{m2} & ar_{m3} \end{bmatrix} \tag{13}$$

式中，$ar_{i1}, i \in [1,m]$ 为备选的第 i 个措施的资源消耗 CON 属性值；$ar_{i2}, i \in [1,m]$ 为备选的第 i 个措施的时间延迟 DEL 属性值；$ar_{i3}, i \in [1,m]$ 为备选的第 i 个措施的安全收益 INC 属性值。

最终确定网络安全防护措施的多属性决策值如式(14)所示。

$$Y = w_1 \cdot \mathrm{CON} + w_2 \cdot \mathrm{DEL} + w_3 \cdot \mathrm{INC} \tag{14}$$

式中，w_1 为资源消耗的权重；w_2 为时间延迟的权重；w_3 为安全收益的权重。

综上所述，本文所提多属性决策模型具有综合性和灵活性等显著特性，其能够综合考虑资源消耗、时间延迟和安全收益等多个评估指标，为复杂决策问题提供全方位的解决方案。此外，该模型通过合理分配各属性权重，平衡安全性与性能需求，并根据不同场景灵活调整，确保在资源受限和实时性要求高的环境中，选择最佳的安全防护措施。

3　实例分析与验证

SCADA 模拟系统如图 2 所示，本文利用服务器、PC 机和 ARM 开发平台模拟搭建 SCADA 系统。以服务器模拟 CCS、PC 机模拟 LCS、ARM 开发平台模拟 RTU、IED 等嵌入式终端设备，通过该模拟系统说明本文所提出的轻量级安全防护措施决策模型的有效性。

双向身份认证备选措施如表 4 所示，RTU 与 LCS 信息加密认证的备选措施如表 5 所示，LCS 与 CCS 之间信息加密认证措施如表 6 所示。

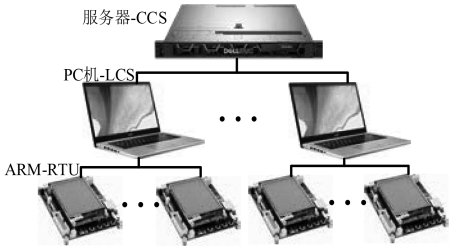

图 2　SCADA 模拟系统

表 4　身份认证备选措施

双向身份认证措施	数字签名算法	Hash 算法
1	SM9 Signature	LHash-64
2	SM9 Signature	U-Quark
3	SM9 Signature	T-Quark
4	ECDSA	LHash-64
5	ECDSA	U-Quark
6	ECDSA	T-Quark

表 5　RTU 与 LCS 信息加密认证备选措施

信息加密认证措施	对称加密算法	Hash 算法
1	DESL	LHash-64
2	DESL	U-Quark
3	DESL	T-Quark
4	PRESENT-80	LHash-64
5	PRESENT-80	U-Quark
6	PRESENT-80	T-Quark
7	KTANTAN-32	LHash-64
8	KTANTAN-32	U-Quark
9	KTANTAN-32	T-Quark

表 6　LCS 与 CCS 信息加密认证备选措施

信息加密认证措施	非对称加密算法	数字签名算法
1	ECC	SM9 Signature
2	SM9	SM9 Signature
3	ECC	ECDSA
4	SM9	ECDSA

本文在 STM32F407 开发平台测试表 4 中双向身份认证措施的资源消耗，包括 CPU 利用率、堆栈利用率和内存占用空间。表 7 为双向身份认证措施的资源消耗测试结果。

在 CPU 利用率方面，第 1 组身份认证措施 CPU 利用率最低，占用了 45%；在堆栈使用率方面，第 3 组身份认证措施堆栈使用率最低，占用了 71%；在内存占用空间方面，

第 1 组身份认证措施最低,为 37.41 kB。

表 7 身份认证措施资源消耗测试结果

安全措施	方案运行时 CPU 利用率/%	方案执行时堆栈使用率/%	内存占用空间/kB
1	45	73	37.41
2	47	74	41.36
3	51	71	39.27
4	59	79	48.50
5	57	77	50.47
6	61	77	47.24

针对长度为 1 000 字节的明文,在 STM32 F407 开发平台测试 Hash 算法和数字签名算法时间延迟,测试结果如表 8 与表 9 所示。由于数字签名算法为非对称密码体制,算法结构复杂,在运行时容易造成较长的安全处理时间延迟,ECDSA 算法完成一次签名生成和还原的时间超过了 100 ms。因此,数字签名仅在通信实时性要求不高的身份认证阶段选用。

表 8 Hash 算法安全处理时间测试结果

Hash 算法	生成摘要时间/ms
LHash-64	0.568 47
U-Quark	0.510 40
T-Quark	0.671 58

表 9 数字签名算法安全处理时间测试结果

数字签名算法	生成与解密签名总时间/ms
ECDSA	130.948 05
SM9 Signature	95.817 85

双向身份认证中使用 Hash 算法和数字签名两种安全措施,根据各措施使用算法摘要长度和签名长度的不同,利用安全收益目标函数计算安全收益,其结果如表 10 所示。

表 10 身份认证安全收益计算结果

身份认证措施	安全收益
1	0.656 249 5
2	0.740 069 5
3	0.811 316 5
4	0.635 099 5
5	0.718 919 5
6	0.790 166 5

根据上述结果建立身份认证措施的决策矩阵并对其归一化处理得到

$$\boldsymbol{DM}_{\text{norm}}=\begin{bmatrix}1 & 0.732\,442\,206 & 0.808\,869\,4\\ 0.170\,330 & 0.732\,765\,752 & 0.912\,182\,9\\ 0.116\,191 & 0.731\,868\,415 & 0.999\,999\,3\\ 0.036\,864 & 0.999\,397\,529 & 0.782\,800\,6\\ 0.040\,940 & 1 & 0.886\,114\,2\\ 0.035\,527 & 0.998\,329\,558 & 0.973\,930\,6\end{bmatrix} \tag{15}$$

双向身份认证措施中,以文献[13]中现场设备安全成本、控制回路安全收益等指标的相对重要程度确定各属性的权重为 $\boldsymbol{W}_{DM}=[0.35,0.1,0.55]^{\mathrm{T}}$,根据权重 $\boldsymbol{W}_{DM}$ 计算出最终的决策结果。

$$\boldsymbol{R}=\begin{bmatrix}0.868\,122\,394\\ 0.634\,592\,466\\ 0.663\,853\,674\\ 0.543\,382\,574\\ 0.601\,691\,696\\ 0.647\,929\,364\end{bmatrix} \tag{16}$$

在 6 种身份认证措施中,第 1 组措施的安全决策计算结果最高,因此身份认证选择第 1 组措施,为 SM9 Signature 和 LHash-64 组合。

对于 RTU 与 LCS 信息加密认证和 LCS 与 CCS 信息加密认证使用同样的方法进行计算,并均以文献[13]中现场设备安全成本、控制回路安全收益等指标的相对重要程度确定 $\boldsymbol{W}_{DM}$。RTU 与 LCS 信息加密认证安全属性权重 $\boldsymbol{W}_{DM}=[0.55,0.2,0.25]^{\mathrm{T}}$,最终确定选择第 7 组措施,为 KTANTAN-32 和 LHash-64 的组合。LCS 与 CCS 的信息加密认证安全属性权重 $\boldsymbol{W}_{DM}=[0.1,0.2,0.7]^{\mathrm{T}}$,最终选择第 2 组措施,为 SM9 和 SM9 Signature 的组合。

至此,本文利用所提出的多属性决策模型完成对双向身份认证措施、RTU 与 LCS 信息加密认证措施和 LCS 与 CCS 信息加密认证措施的优选。模型通过综合考虑资源消耗、时间延迟和安全收益等因素,确保选取的安全措施在最小化资源占用的同时,满足实时性需求,并在安全性与性能之间达到最优平衡,验证了“轻量级安全防护措施决策模型”在 SCADA 系统中的有效性。

4 结束语

本文构建了基于多属性决策的轻量级防护措施决策模型,该模型引入资源消耗、时间延迟和安全收益 3 个属性建立属性目标函数,并根据层次分析法计算各属性目标函数的权重得到决策函数建立决策矩阵。针对所提出安全防护方案,在模拟系统中测试安全防护方案中各组防护措施资源消耗及时间延迟指标,并计算防护措施的安全收益,根据不同防护措施的安全属性权重,计算各组备选措施决策值,最终确定轻量级防护措施。于搭建的模拟 SCADA 系统中使用所提模型对算例进行分析,验证结果表明所提模型能实现备选措施的优选。

参考文献

[1] 叶剑斌, 左剑飞, 黄小鈥. 群远程集中 SCADA 系统设计[J]. 电力系统自动化, 2010, 34(23):97-101.

[2] 罗新宇. SCADA 系统信息安全评估与智能防护研究[D]. 湘潭:湘潭大学, 2021.

[3] 邓力. SCADA 系统信息安全防护技术研究[D]. 成都:电子科技大学, 2017.

[4] ALVES T, DAS R, MORRIS T. Embedding encryption and machine learning intrusi on prevention systems on programmable logic controllers[J]. IEEE Embedded Syst ems Letters, 2018, 10(3):99-102.

(下转第 167 页)