

电力监控系统网络安全态势感知研究

成 健¹, 胡力广¹, 詹威鹏¹, 陈腾彪¹, 孙 凤²

(1. 深圳供电局有限公司, 广东 深圳 518020; 2. 深圳市深鹏达电网科技有限公司, 广东 深圳 518020)

摘要: 由于传统态势感知方法在进行电力监控系统网络安全态势感知时对安全态势值的计算不精准, 导致感知风险传播衰减率与实际风险传播衰减率相比误差较大, 无法实现对电力监控系统网络安全态势的精准感知。针对这一问题, 进行电力监控系统网络安全态势感知研究。通过转换网络安全态势映射, 输出可供计算的网络安全态势映射, 为计算安全态势值提供数据支持; 计算安全态势值, 得出电力监控系统网络安全态势值的取值范围为 $[0,1]$, 数值越大证明该电力监控系统受到网络攻击的可能性就越高。实验结果表明, 设计的态势感知方法感知风险传播衰减率与实际风险传播衰减率最大误差不超过 ± 0.004 , 实验对照组最大误差为 ± 0.308 , 设计态势感知方法可以实现对电力监控系统网络安全态势的精准感知。
关键词: 电力监控系统; 网络安全; 态势感知; 安全态势值

Research on network security situation awareness of power monitoring system

CHENG Jian¹, HU Liguang¹, ZHAN Weipeng¹, CHEN Tengbiao¹, SUN Feng²

(1. Shenzhen Electricity Supply Bureau Co., Ltd., Shenzhen 518020, China; 2. Shenzhen Splendor Power Grid Technology Co., Ltd., Shenzhen 518020, China)

Abstract: Due to the traditional situation awareness method, the calculation of the security situation value is not accurate in the process of network security situation awareness of power monitoring system, resulting in a large error between the perceived risk propagation attenuation rate and the actual risk propagation attenuation rate, which can not realize the accurate perception of the network security situation of power monitoring system. In order to solve this problem, the network security situation awareness of power monitoring system is studied. Through the transformation of network security situation mapping, the available network security situation mapping is output to provide data support for the calculation of security situation value; the security situation value is calculated, the value range of the power monitoring system network security situation value is $[0,1]$ is got. The larger the value, the higher the possibility of the power monitoring system being attacked by the network. The experimental results show that the maximum error between the perceived risk propagation attenuation rate and the actual risk propagation attenuation rate of the designed situation awareness method is not more than ± 0.004 , and the maximum error of the experimental control group is ± 0.308 . The designed situation awareness method can realize the accurate awareness of the network security situation of the power monitoring system.

Key words: power monitoring system; network security; situation awareness; security situation value

0 引言

传统网络安全态势感知方法在实际运行过程中, 容易出现影响电力监控系统网络安全的

问题^[1]。这种情况下, 不但会影响电力监控系统网络运行环境, 甚至还会导致经济方面的损失。传统网络安全态势感知方法主要出现的网

络安全问题包括网络恶意攻击、植入恶意病毒以及程序恶意破坏^[2]。当网络安全态势感知方法遭受种种原因而崩溃时,对于电力监控系统网络安全态势进行提前预测是解决此问题最有效的方式。电力监控系统是确保供电安全,并保证电力信息不受到恶意攻击的有效手段。因此,本文通过电力监控系统网络安全态势感知研究,致力于基于网络安全态势感知改变传统电力监控系统自动感知要素^[3]。通过神经网络整合自动感知网络安全态势的方式实现节本增效,从根本上提高网络安全态势感知风险传播衰减率。

1 电力监控系统网络安全态势感知方法

所设计的电力监控系统网络安全态势感知方法可分为三层架构,分别为安全态势预测、安全态势要素提取以及安全态势理解,逐一实现电力监控系统网络安全态势感知。本文通过三步运算,实现电力监控系统网络安全态势感知。针对态势预测进行网络安全态势映射转换;通过计算安全态势值,提取态势要素;感知安全态势值灰色关联度,完成态势理解。针对以上三步运算的具体阐述如下。

1.1 转换网络安全态势映射

将电力监控系统看作是一个有机整体,而电力监控系统网络中的信息元素之间存在关联性^[4]。这就意味着,某个元素的网络安全态势风险可以通过这种关联性传播到下一个元素中。因此,电力监控系统网络安全态势安全预测就是通过对这种关联性传播进行预测的,本文设计的电力监控系统网络安全态势安全预测流程如下图所示。

图中,设 u 为电力监控系统中所有主机的集合,对预测到的未来安全态势值映射进行转换^[5]。由于电力监控系统网络安全态势值映射是一个累加值,随时会由于受到不同程度的网络攻击而产生剧烈的波动。因此,转换网络安全态势映射函数必须建立在提高对电力监控系

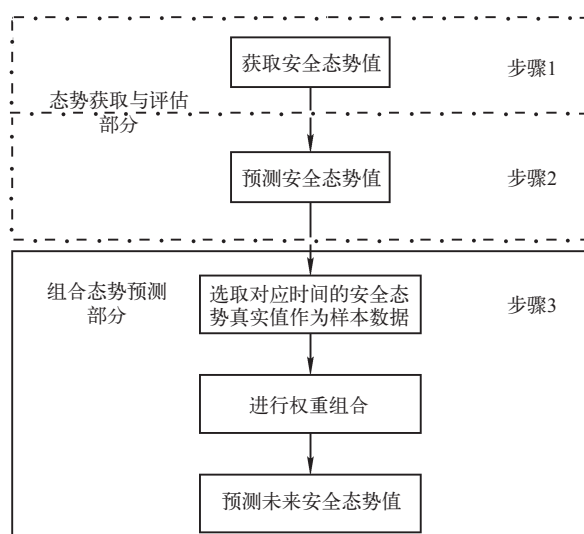


图 电力监控系统网络安全态势安全预测流程

Fig. Network security situation security prediction process of power monitoring system

统网络安全态势感知敏感性的基础上,本文选用 $\arctan(x)$ 函数作为转换网络安全态势映射的目标函数,其算法为

$$NET_X = \frac{\arctan(NET_F)}{\frac{\pi}{2}} \quad (1)$$

式中, NET_X 为转换后的网络安全态势映射参数; NET_F 为转换前的网络安全态势映射参数。

通过式(1)完成网络安全态势映射转换后,输出可供计算的网络安全态势映射,为计算安全态势值提供数据支持。

1.2 计算安全态势值

电力监控系统在运行过程中,必然会面临潜在的风险,由于风险系数不同,其网络安全态势的重要性也各有不同^[6]。因此,本文通过计算安全态势值,对不同网络安全态势的重要性以及破坏程度进行分析。设 j 类受到的网络攻击表示为 a_j ,则 $0 \leq a_j \leq 1$; i 网络安全态势的重要性表示为 β_i ,则 $0 \leq \beta_i \leq 1$;而 x_i 为电力监控系统正常情况下主机检测的网络安全态势抗体数量; n_i 为电力监控系统时刻检测的网络安全态势抗体数量; n_{ij} 为电力监控系统处

理网络攻击时的抗体数量。假定 $r_i(t)$ 为电力监控系统在 t 时间段的安全态势值,则其计算公式为

$$r_i(t) = 1 - (1 / 1 + \ln(\beta_i(n_i - x_i) + 1)) \quad (2)$$

在式(2)的基础上,设电力监控系统在 t 时间段受到 j 类网络攻击的安全态势值为 $r_{ij}(t)$,则其计算公式为

$$r_{ij}(t) = 1 - (1 / 1 + \ln(a_j \beta_i(n_{ij} - x_i) + 1)) \quad (3)$$

通过式(3)可以得出,电力监控系统网络安全态势值的取值范围为 $[0, 1]$,数值越大,证明该电力监控系统受到网络攻击的可能性越高^[7]。

1.3 感知安全态势值灰色关联度

得到安全态势值后,本文采用灰色关联度的方式对安全态势值进行感知^[8]。根据灰色关联度定义,感知电力监控系统中的网络安全因素在时间及其他变量发生变化过程中的相关性度量。相关性度量可通过以下数列进行实现,即 $x_0 = \{x_0(t) | t = 1, 2, \dots, n\} = \{x_0(1), x_0(2), \dots, x_0(n)\}$ (4)

根据式(3),假设电力监控系统网络安全态势有 m 个对比数列,那么式(4)可写成 $x_i = \{x_i(1), x_i(2), \dots, x_i(n)\} = P(0, 1), i = 1, 2, \dots, m$ (5) 式中, $P(0, 1)$ 为安全态势值灰色关联度分辨系数, P 数值越大,证明该电力监控系统网络安全态势感知分辨率就越大。

因此,可以得到

$$r_i = (1 / P) \sum \psi_i(t) \quad (6)$$

式中, r_i 为感知到的安全态势值灰色关联度; ψ 为关联度权重。

通过式(6)可以对电力监控系统网络安全态势进行综合感知。为确保感知安全态势值灰色关联度过程中不会出现信息丢失的情况,将网络安全态势自动感知偏差值设为 x ,可得 x 的计算公式为

$$x = \frac{r}{B^d} \quad (7)$$

式中, r 为网络安全态势自动感知态势值; d 为网络安全态势自动感知特征维数; B 为网络安全态

势自动感知的逻辑矢量。

电力监控系统网络安全态势感知的实现,意味着能够基于电力监控系统网络安全态势感知方法实现自动感知功能。

2 实验分析

2.1 实验准备

构建实验,在网络中设置一台漏洞扫描设备作为攻击源模拟网络攻击行为,实验对象选取某电力监控系统,并对网络攻击行为参数进行具体设计。网络攻击行为具体参数如表1所示。

表1 网络攻击行为参数

Tab. 1 Network attack behavior parameters

攻击指令	弱点标识	被攻击ID	时刻
Ghfgsdpa	BTY - 2001 - 1547	171.11.15 2.45	00:10:08
hjsosavg	BTY - 2002 - 3675	171.11.15 4.50	00:15:21
ydhaiavnsax	BTY - 2003 - 2457	171.11.15 4.45	00:08:26
hiafjaivsa	BTY - 2004 - 3747	171.11.15 2.100	00:04:38
fgwusfgrfg	BTY - 2004 - 8456	171.11.15 3.100	00:05:30
thuehacv	BTY - 2005 - 1348	171.11.15 1.100	00:11:50
rthbihsavg	BTY - 2005 - 8675	171.11.15 3.150	00:15:42

根据表1,分别使用传统态势感知方法以及本文设计的态势感知方法进行实验,设置传统的态势感知方法为实验对照组。本次设计的仿真实验硬环境包括处理器Inter(R) Core(TM) Duo CPU、支持8线双绞线同轴电缆光纤专网、CPRS/DCMA无线公网以及无线专网;仿真实验软件为MapReduce编程框架,主要用于对网络安全态势感知数据集成的仿真模拟,并且能够完成数据统计任务。实验主要内容为核查两种态势感知方法的感知风险传播衰减率,感知风险传播衰减率与实际风险传播衰减率数值越接近,证明该感知方法的感知准确度越高。在此次实验中共进行10次实验。针对MapReduce测得的风险传播衰减率,记录实验结果,进而判断两种态势感知方法的准确度。

2.2 实验结果分析与结论

根据上述设计的实验步骤,采集10组实验数据,将两种态势感知方法下的感知风险传播衰减率与实际风险传播衰减率进行对比。并将感知风险传播衰减率对比结果导入MapReduce编程框架,以表格的形式进行展示,具体结果如表2所示。

表2 感知风险传播衰减率对比

Tab. 2 Comparison of perceived risk propagation attenuation rate (%)

实验次数	设计方法感知风险传播衰减率	对照组感知风险传播衰减率	实际风险传播衰减率
1	0.254	0.374	0.250
2	0.253	0.378	0.250
3	0.254	0.369	0.250
4	0.251	0.357	0.250
5	0.248	0.374	0.250
6	0.249	0.558	0.250
7	0.250	0.514	0.250
8	0.247	0.538	0.250
9	0.252	0.547	0.250
10	0.250	0.452	0.250

通过表2可知,本文设计的态势感知方法感知风险传播衰减率与实际风险传播衰减率最大误差不超过 ± 0.004 ,实验对照组最大误差为 ± 0.308 ,设计态势感知方法可以实现对电力监控系统网络安全态势的精准感知。通过仿真验证结果证明,所设计的态势感知方法其各项功能均可以满足施工总体要求,可以广泛应用于电力监控系统网络安全态势感知领域。

3 结束语

本文对电力监控系统网络安全态势感知进行了研究,通过提出一种新的电力监控系统网络安全态势感知方法,提高了电力监控系统网络安全态势感知的准确度。由于此次研究时间有限,虽然取得了一定的研究成果,但对于该方法的研究仍有不足,今后还要对其进行进一步研究,为电力监控系统网络安全态势感知方法的进一步优化提供参考依据。通过仿真实验证明,所设计的态势感知方法在降低感知误差方面的具体优势已经显现出来。但本文唯一不足之

处在于,没有针对电力监控系统网络安全态势感知模型进行设计,这一点可以作为电力监控系统网络安全态势感知领域在日后的研究方向。

参考文献

- [1] 李腾飞,李强,余祥,等.基于拓扑漏洞分析的网络安全态势感知模型[J].计算机应用,2018,38(增刊2):162-168,174.
- [2] 刘世文,马多耀,雷程,等.基于网络安全态势感知的主动防御技术研究[J].计算机工程与科学,2018,40(6):102-109.
- [3] 赖积保,王颖,王慧强,等.基于多源异构传感器的网络安全态势感知系统结构研究[J].计算机科学,2011(3):150-155,164.
- [4] 惠馨雅,刘建华,刘浩.基于有色Petri网的网络安全态势感知模型构建及分析[J].计算机与数字工程,2019,47(2):393-396,401.
- [5] 胡建平,郝惠英,张学高,等.卫生健康行业网络安全态势感知平台建设探讨[J].中国卫生信息管理杂志,2019,16(1):4-8.
- [6] 蔡梓文,杨劲锋,廖年冬,等.基于模糊推理的计量自动化系统网络安全态势感知[J].南方电网技术,2019,13(2):51-58.
- [7] 韩晓露,刘云,张振江,等.网络安全态势感知理论与技术综述及难点问题研究[J].信息安全与通信保密,2019(7):61-71.
- [8] 邓文信.一种基于多协议的粮食港区电力监控系统的设计与应用[J].计算机应用与软件,2019,36(1):180-184,190.

作者简介



成 健

成健(1989-),男,工程师,主要研究方向为输电缆运维管理及智能技术应用。

(收稿日期:2020-03-16)EA