引用本文：李子凡，张永壮，陈芳，等. 拟态 SDON 传输系统中冗余异构多核架构的实现[J]. 光通信技术，2022，46(1)：81–85.

拟态 SDON 传输系统中冗余异构多核架构的实现

李子凡[1]，张永壮[2]，陈 芳[1]，陈方正[1]，田 元[1]，田照宇[1]，钱升起[1]，赵星宇[1]，李 欣[2]，张会彬[2]

（1.国家电网有限公司 信息通信分公司，北京 100053；2.北京邮电大学 电子工程学院，北京 100876）

摘要：现有增强光传输网络安全性的方法多是基于网络层面的，无法保障光传输设备的安全性。提出在光传输设备的管理控制系统中引入拟态防御技术，设计了设备的冗余异构多核架构。基于系统相似度构建攻击概率模型，并进行仿真验证。结果表明：所提方法明显降低了系统被攻击成功的概率，大大提高了拟态软件定义光网络传输系统的安全性能。

关键词：多核；冗余异构；软件定义光网络；光传输设备；安全增益

中图分类号：TN914　**文献标志码**：A　**文章编号**：1002-5561(2022)01-0081-05

DOI：10.13921/j.cnki.issn1002–5561.2022.01.017　**开放科学(资源服务)标识码(OSID)**：

Implementation of redundant heterogeneous multi–core architecture in Mimic SDON transmission system

LI Zifan[1], ZHANG Yongzhuang[2], CHEN Fang[1], CHEN Fangzheng[1], TIAN Yuan[1], TIAN Zhaoyu[1], QIAN Shengqi[1], ZHAO Xingyu[1], LI Xin[2], ZHANG Huibin[2]

(1. State Grid Information & Telecommunication Branch, Beijing 100053, China;
2. School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Most of the existing methods to enhance the security of optical transmission network are based on the network level and cannot guarantee the security of optical transmission equipment, this paper proposes to introduce the pseudo defense technology into the management and control system of optical transmission equipment, and designs a redundant heterogeneous multi-core architecture. Based on the system similarity, the attack probability model is constructed and verified by simulation. The results show that the proposed method significantly reduces the probability of successful attack and greatly improves the security performance of pseudo software defined optical network transmission system.

Key words: multi-core, redundant heterogeneous, software defined optical network, optical transmission equipment, security gain

0 引言

软件定义光网络(SDON)是软件定义网络与传统光传输网络的结合，可以实现控制平面与数据平面的解耦，使得远程控制器可以配置来自不同硬件供应商的网络设备[1]。SDON 结合了在光层中优化特定网络碎片化和业务高带宽的优点，为不同网络提供了统一的控制平台[2]。但是，SDON 安全性较差，面临信息泄露和网络瘫痪的风险。已有大量文献研究了增强 SDON 系统安全性的方法，如分布式控制器[3]、弹性控制平面[4]、SDON 控制器上的拟态防御[5]和虚拟服务链[6]等，但这些方法主要聚焦在提高控制层的安全性，很少考虑物理层的安全性。基于此，本文提出一种在拟态 SDON 传输系统光传输设备中实现的冗余异构多核架构。

收稿日期：2021–05–08。

作者简介：李子凡(1990—)，男，博士，目前就职于国家电网有限公司信息通信分公司，主要研究方向包括电力通信网、光传输网络、无线通信和网络管理，曾参与研究国家电网有限公司信息通信分公司自建科技项目“光纤智能运维检测系统研究与应用”。

1 系统架构

1.1 拟态 SDON 传输系统

图 1 为拟态 SDON 传输系统的架构图，该系统分为应用层、控制层和物理层三部分。应用层收集 SDON 控制器信息并显示图形界面；控制层实现对网络资源的集中控制；物理层主要由拟态 SDON 传输设备组成。其中，拟态 SDON 传输设备具有外部接口，即管控接口和线路层接口：在光传输设备开发 SDON 管控接口，通过交换机相连实现与控制层的通信；在开发

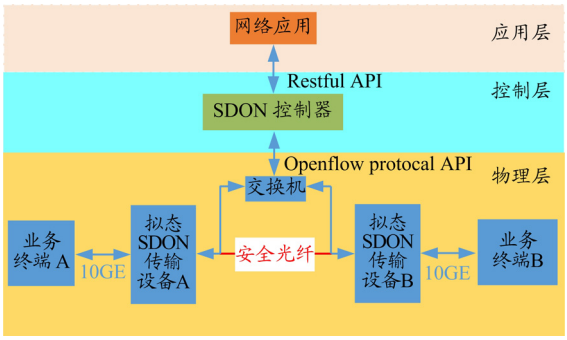
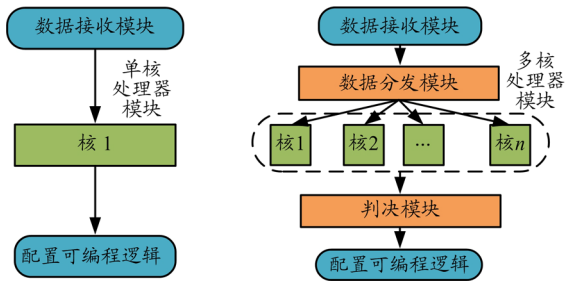


图 1 拟态 SDON 传输系统架构图

SDON 线路层接口,实现光传输设备之间的连接。本文通过在拟态 SDON 传输设备中实现冗余异构多核架构来提高系统的安全性。

1.2 多核架构模型

光传输设备的单核架构流程图如图 2(a)所示,传统单核系统只有一个核作为处理器。单核处理器处理完数据后把结果发送到光传输设备进行配置。由于单核系统结构简单,在遭受攻击后无法确定数据的正确性。光传输设备冗余异构多核架构流程图如图 2(b)所示,冗余异构多核架构由数据接收模块、数据分发模块、多核处理器模块和判决模块 4 个模块组成。数据接收模块采用 SDON 管控接口接收控制层下发的数据;数据分发模块复制这些数据并将它们发送给多核处理器模块;多核处理器模块是系统的核心;判决模块基于大数判决算法来裁决多核处理器的处理结果。



(a) 单核架构流程图　　(b) 冗余异构多核架构流程图

图 2 光传输设备架构

在一个冗余异构系统中,执行体是指一组功能等价的组件[7],异构性是指在不同结构构造的执行体上实现相同功能的组件。本文设计的拟态 SDON 传输系统中光传输设备的异构性可分为 2 个层面:硬件层面上多核冗余异构和软件层面上的核上算法异构。多核架构框图如图 3 所示,该架构包含加速处理器和无线电处理器两部分。处理系统(PS)上有 2 种 Arm 类型的核:64bit 的 Cortex-A53 核和 32bit 的 Cortex-R5 核。该

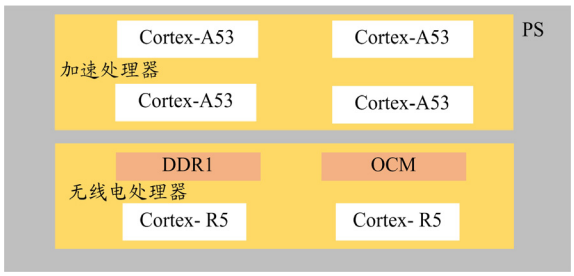


图 3 多核架构框图

系统使用 4 个 Cortex-A53 核和 2 个 Cortex-R5 核来构建硬件层面上的冗余异构执行体,使用不同的核上算法构建软件层面的冗余异构执行体。共享内存双倍速率(DDR)同步动态随机存储器和片上存储器(OCM)实现多核处理器间的通信、中断和轮询,在多核处理器间实现信息交互。

2 安全性分析

2.1 系统相似度

在一个冗余异构系统中,执行体包含几个组件。对于一个有 n 个执行体的系统来说,第 k 个组件的特征相似矩阵为[8]:

$$A_k=\begin{bmatrix} 1 & \delta_{12}^k & \delta_{13}^k & \cdots & \delta_{1n}^k \\ \delta_{21}^k & 1 & \delta_{23}^k & \cdots & \delta_{2n}^k \\ \delta_{31}^k & \delta_{32}^k & 1 & \cdots & \delta_{3n}^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \delta_{n1}^k & \delta_{n2}^k & \delta_{n3}^k & \cdots & 1 \end{bmatrix} \tag{1}$$

其中,A_k 是相似矩阵,δ_{ij}^k $(0<i\neq j\leqslant s, 0<\delta_{ij}\leqslant 1)$代表第 k 个组件中的第 i 个和第 j 个类目的相似度。冗余异构系统的相似度是不同组件相似度的加权和[9],即

$$A=\sum_{k=1}^{m}\omega_k A_k \tag{2}$$

其中,A 是整个系统的特征相似矩阵,ω_k 是相似权重,m 是组件的数量。

拟态 SDON 传输系统的执行体组件包含 2 种:硬件和软件。硬件层面的漏洞比软件层面多。因此,本文设置硬件相似度权重为 0.7,软件相似度权重为 0.3。冗余异构系统的相似度是所有不同元素的相似度之和的归一化[8],可以用式(3)表示。

$$H_n=\frac{1}{\alpha_n}=\frac{C_n^2}{\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\delta_{ij}}, 0<\alpha_n\leqslant 1 \tag{3}$$

其中,δ_{ij} 代表整个系统中第 i 个和第 j 个执行体的相似度,α_n 代表有 n 个执行体的系统相似度。H_n 为系统的异构程度,当系统中所有执行体构造相同时,相似度为 1;当系统中执行体间的构造差别越大时,相似度越趋近于 0。因此,H_n 和 α_n 的值成反比。

2.2 攻击概率模型

若攻击能力用攻击者攻击成功的概率密度函数来描述,记为 $v(t)$,则攻击者在时间 t 内攻击成功概率记为 $P=\int v(t)\mathrm{d}t$。若攻击者对同一目标依次发起了 n 次攻击,则每次攻击的持续时长均为 t,攻击成功的概率分别为 P_1, P_2, …, P_n,若 $\forall i、j,\Rightarrow P_i=P_j$,且与时间无关,则称攻击者的攻击能力是无记忆的,否则,为有记忆的;若在任意的攻击周期内,$v(t)$ 和时间无关,即 $\forall t_1\neq t_2,\Rightarrow v(t_1)=v(t_2)$,则称攻击能力是非时变的,否则是时变的。

在物理层面上,$v(t)$描述了攻击成功概率的变化速率,即单位时间内攻击成功概率的分布。本文假设无记忆非时间的攻击者为攻击源,选取指数分布函数来刻画攻击者的攻击能力,则执行体在单次持续攻击下的攻击成功概率为[10]:

$$P_i(t)=\int v(t)\mathrm{d}t=\int \lambda e^{-\lambda t}\mathrm{d}t \tag{4}$$

其中,λ 是一个常数,本文设 λ=0.3。

根据经验判决原则:当执行体数量为奇数时,判决算法的准确性更高。因此,为确保大数判决算法的准确性,设执行体的数量为奇数,即 $n=2k+1(k=0,1,2\cdots)$。本文将系统相似度 α_n 的值定义为影响攻击者攻击成功概率的随机影响因子,假设攻击者对每个执行体有相同的攻击概率,安全性能的差异性由随机影响因子来描述,则对于一个有 n 个执行体的冗余异构系统,系统被攻击成功的概率[11]可以表示为:

$$P_n(t)=\alpha_n\sum_{k=(n+1)/2}^{n}p_i^k(1-p_i)^{n-k} \tag{5}$$

对于防御者来说,攻击者未能成功攻击系统的概率反应了它的安全性能。因此,拥有 n 个执行体的系统的安全增益为:

$$\Delta_n(t)=\frac{1-P_n(t)}{1-P_1(t)} \tag{6}$$

2.3 执行体的选择

本文使用微软公司开发的 MOSS 工具来测量不同核上算法之间的相似度。因为相似度在硬件层面上测量难度较大,所以设置 Cortex-A53 和 Cortex-R5 核的硬件相似度为 0.65,代表着一个中等相似度水平。

本文仅考虑光传输设备在单核、三核和五核情况下的异构执行体。当光传输设备仅仅有一个执行体时,α_1=1,H_1=1。为了保证执行体集合异构度越大,相似度越低,应保证执行体集合中的执行体尽可能异构。假设 A53-m_1(m_1=0,1,2),R5-m_2(m_2=0,1)分别表示 Cortex-A53 和 Cortex-R5 核的编号,选取三核执行集为{A53-0,A53-1,R5-0},相似度矩阵如下:

$$A_1=\begin{bmatrix}1&1&0.65\\1&1&0.65\\0.65&0.65&1\end{bmatrix},A_2=\begin{bmatrix}1&0.233&0.300\\0.233&1&0.240\\0.300&0.240&1\end{bmatrix},$$

$$A=\begin{bmatrix}1&0.770&0.521\\0.770&1&0.512\\0.545&0.527&1\end{bmatrix}。$$

根据式(3)可知,α_3=0.614 时,H_3=1.629。

五核执行体集合为{A53-0, A53-1,A53-2,R5-0, R5-1},相似度矩阵如下:

$$A_1=\begin{bmatrix}1&1&1&0.65&0.65\\1&1&1&0.65&0.65\\1&1&1&0.65&0.65\\0.65&0.65&0.65&1&1\\0.65&0.65&0.65&1&1\end{bmatrix},$$

$$A_2=\begin{bmatrix}1&0.770&0.773&0.545&0.515\\0.770&1&0.786&0.527&0.512\\0.773&0.786&1&0.571&0.536\\0.545&0.527&0.571&1&0.768\\0.515&0.512&0.536&0.786&1\end{bmatrix},$$

$$A=\begin{bmatrix}1&0.770&0.773&0.545&0.515\\0.770&1&0.786&0.527&0.512\\0.773&0.786&1&0.571&0.536\\0.545&0.527&0.571&1&0.786\\0.515&0.512&0.536&0.786&1\end{bmatrix}。$$

根据式(3)可知,α_5=0.630 时,H_5=1.587。

综上所述,相比单核系统,三核和五核系统的异构程度得到巨大提升。然而,由于五核系统的执行体相似数量多,五核系统的异构程度会略低于三核系统。

3 仿真和数据分析

本文基于 Matlab 平台上的 plot 函数仿真得出理论分析的攻击概率与安全增益图像。拟态 SDON 传输设备内部实物图如图 4 所示,包含电源模块、激光模块和主模块,攻击成功概率随单次攻击持续时间的变

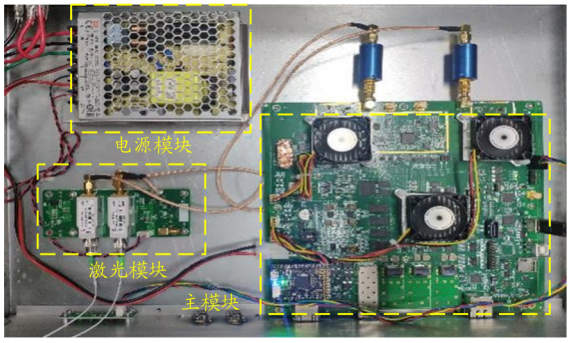


图 4 拟态 SDON 传输设备内部架构图

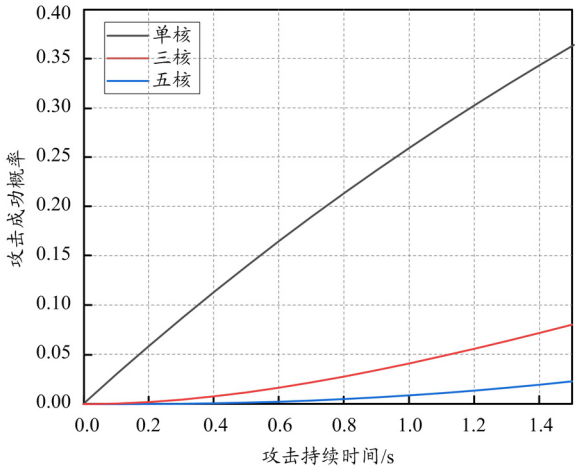


图 5 攻击概率图

化如图 5 所示,安全增益随单次攻击持续时间的变化如图 6 所示。本文截取几个时间节点下的系统被攻击成功的概率和安全增益值,如表 1 所示。

仿真结果显示多核系统被成功攻击的概率远低于单核系统,安全增益相比单核系统(其安全增益在持续时间下默认为 1)也得到明显提升。此外,在相同的攻击持续时间下,相比三核系统,五核系统被成功攻击的概率较低,安全增益较高。

在接收数据量和其它软硬件设备不变的情况下,本文分别测量光传输系统在单核、三核和五核情况下的运行时间如图 7 所示。单核系统的最大核运行时间为 26.55 ms,三核系统的最大核运行时间为 60.21 ms,五核系统的最大核运行时间为 74.34 ms;多核系统的数据复制分发时间很低,几乎可以忽略不计;与单核处理器相比,多核系统的总运行时间主要在于最大核运行时间、读取共享内存寄存器时间和大数判决算法时间,其中最大核运行时间取决于所有核中运行时间最长的核,即算法时间复杂度最高的核;五核系统读取寄存器的时间略高于三核系统,这是因为五核系统收发数据时读取寄存器的数量变多,但读取每个寄存

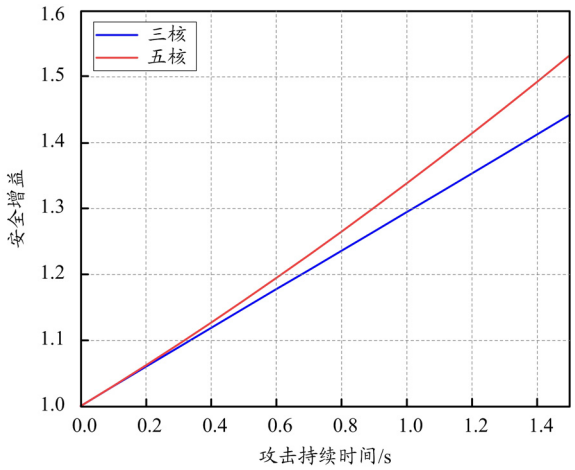


图 6 安全增益图

表 1 攻击成功概率和安全增益值

持续时间	$P_1(t)$	$P_3(t)$	$\Delta_3(t)$	$P_5(t)$	$\Delta_5(t)$
0.5	13.93%	3.24%	1.125	1.37%	1.147
1	25.92%	10.24%	1.215	7.15%	1.257
1.5	36.24%	18.34%	1.287	16.05%	1.326

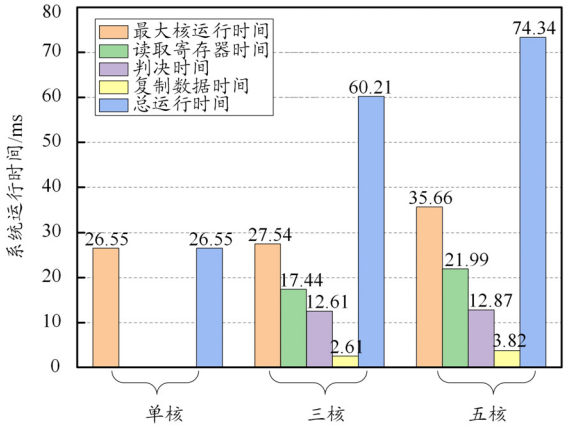


图 7 多核系统的运行时间

器的时间较短;而三核系统和五核系统的判决时间大致相等,这是因为判决算法在裁决时时数据量较小,对整体判决时间影响很小。

结合表 1 和图 7 可知,三核系统的运行时间是单核系统的 2.27 倍,五核系统的运行时间是单核系统的 2.8 倍。当攻击持续时间为 0.5 s 时(常用攻击源),单核系统被成功攻击的概率是 13.93%,三核系统被成功攻击的概率是 3.24%,五核系统被成功攻击的概率是 1.37%。此时,三核系统的安全增益是 1.125,五核系统的安全增益是 1.147。

4 结束语

本文在拟态 SDON 传输系统中设计并实现了冗余异构多核架构,在理论上分析了相似度、异构度、攻击成功概率和安全增益等影响系统安全性能的参数,测量了不同的单次攻击持续时间时的单核和多核系统的攻击概率和安全增益。使用 Matlab 软件仿真,分别得出单核和多核系统的攻击成功概率和安全增益图像,并截取某几个时间点,计算出单核和多核系统的攻击成功概率和安全增益值。仿真结果显示:多核系统的异构度和安全性能远高于单核系统,且五核系统的安全性能优于三核系统,说明本文的设计能显著提升 SDON 传输系统物理层的安全性。此外,由于系统设计时未引入额外的硬件,所以成本很低,实现相对简单。

参考文献:

[1] YANG H, ZHAO X D, YAO Q Y, et al. Accurate fault location using deep neural evolution network in cloud data center interconnection [EB/OL]. [2021-05-08]. https://ieeexplore.ieee.org/document/9000910.

[2] YANG H, YU A, ZHANG J, et al. Data-driven network slicing from core to RAN for 5G broadcasting services[J]. IEEE Transactions on Broadcasting, 2021, 67(1): 23–32.

[3] 徐云斌,纪雨彤,赵星,等. 软件定义光网络中基于控制器的多域协同恢复机制[J]. 光通信技术,2018,42(12):47–50.

[4] CHEN Y Y, LI Q, YANG Y, et al. Towards adaptive elastic distributed software defined networking[C]// International Performance Computing and Communications Conference, December 14–16, Nanjing, China. Nanjing: IEEE, 2015: 1–8.

[5] 李堃,欧清海,刘柱,等. 基于控制器集群的 SDON 多域互联互通技术[J]. 光通信技术,2017,41(9):9–12.

[6] YANG H, ZHANG J, ZHAO Y L, et al. CSO: cross stratum optimization for optical as a service [J]. IEEE Communications Magazine, 2015, 53(8): 130–139.

[7] 王晶,欧清海,廖道,等. 多层异构软件定义光网络协同互联方法[J]. 光通信技术,2017,41(7):1–4.

[8] 刘勤让,林森杰,顾泽宇. 面向拟态安全防御的异构功能等价体调度算法[J]. 通信学报,2018,39(7):188–198.

[9] 张杰鑫,庞建民,张铮,等. 面向拟态构造 Web 服务器的执行体调度算法[J]. 计算机工程,2019,45(8):14–21.

[10] 扈红超,陈福才,王禛鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报,2016,1(4):40–51.

[11] 樊永文,朱维军,班绍桓,等. 动态异构冗余数据保护安全架构[J]. 小型微型计算机系统,2019,40(9):1956–1961.