一种 FC 交换式网络节点机信任管理方法

张奕然[1] 曹 月[1] 步京蓬[2] 马艺新[1]
ZHANG Yiran CAO Yue BU Jingpeng MA Yixin

摘 要 伴随着计算机系统对高速数据大量传输的需求，美国国家标准委员会提出具有高带宽、低延迟、灵活的 FC（光纤通道协议），但光纤存储网络可以存储大量数据的同时，也存在着数据信息安全隐患问题。当网络中的节点机被外部或内部攻击节点攻击后，便会造成整个网络中的安全隐私数据存在泄露的风险。针对上述问题，提出一种 FC 交换式网络信任模型，并将其应用于节点机的信任管理模块中。实验测试结果表明，所提出的模型可以将综合信任值小于信任阈值的恶意节点机从 FC 网络中剔除，提高 FC 网络的安全性。

关键词 FC 网络；信任模型；网络安全；信任管理；恶意节点剔除

doi：10.3969/j.issn.1672-9528.2024.03.044

0 引言

FC（光纤通道协议）[1] 由美国国家标准委员会提出，最初是为了解决 I/O 传输瓶颈对整个存储系统带来的消极影响，从而形成了一个光纤通道标准协议簇，再加上 FC 网络的高带宽、低延迟、低位错率、灵活的拓扑结构，FC 网络已经在信息存储、银行、电信、广播、电视、工业仪器等领域广泛使用，并逐渐开始在航空、军事、工业实时控制等领域应用。

在光纤网络中，基本的拓扑结构有点对点、仲裁环、交换式三种。与传统的千兆以太网对比，虽然交换式的组网结构和以太网类似，但是 FC 网络具备有传统以太网不具备的如支持多种上层协议、支持多种底层传输介质、支持基于信用的流量控制等特点，再加上支持的 16 Gbit/s 以上的链路速率，支持多种拓扑结构，已经在组网选择的过程中具备绝对优势。

然而，光纤存储网络可以存储大量数据的同时，也存在着数据信息安全 [2] 隐患问题，所以信息安全问题也是 FC 网络中关键的一环。常见的安全技术手段有数据加密和访问控制表等。在交换式 FC 网络中，每台节点机设备及交换机设备都有其唯一的端口号，消息的收发也都是通过端口来进行的，所以说端口对于节点的安全性尤为重要。当发送节点机被恶意捕获 [3] 时，会导致端口发送给交换机的信息丢失或者被篡改；当交换机节点被捕获时，可能会导致交换机端口发送给全网的消息出现混乱，消息无法正常收发。

1. 航空工业计算所 陕西西安 710068
2. 中航西安飞机工业集团股份有限公司 陕西西安 710089

1 FC 交换式网络系统架构

FC 交换式网络 [4] 系统架构如图 1 所示，FC 交换网络中的设备通过光纤相连接，有交换机和节点机两种设备，其中交换机被称为 F 端口，节点机被称为 N 端口，一个或多个节点机通过光纤接在交换机的不同端口上，节点机端口与交换机端口相连进行信息交互。

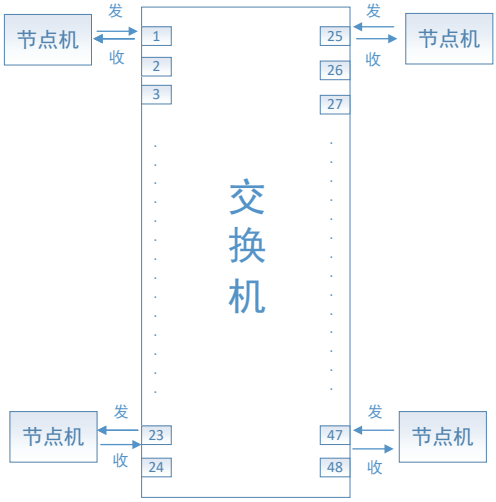

图 1 FC 交换式网络系统架构

2 信任模型设计

本文引入的信任模型是假设 FC 网络中的交换机端口均为安全可信端口，引入信任模型的主要目的是识别并剔除通过隐私泄露、拒绝服务、消息篡改伪造、身份假冒等攻击方式成为恶意节点的网络节点机成员。为了防止光纤通信网络中可能存在的恶意节点机接入整个网络，提出带有恶意行为

监测的信任模型，对存在异常行为的节点机进行识别隔离。针对光纤通信交换式网络存在的安全威胁，以信息交互过程中的节点行为和交互成功率作为信任因子[5]，同时结合空间和时间维度，得到节点机的直接信任度、间接信任度和历史信任度，节点机信任度表如图2，节点机信任模型如图3，再通过聚合求得综合信任度，对邻居节点机的行为进行信任度评估。

图2 节点机信任度表

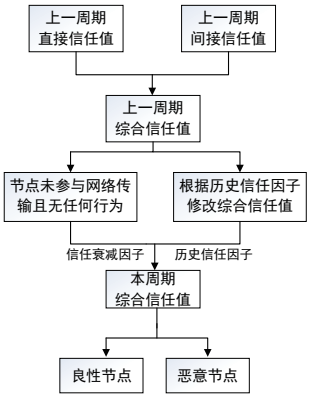

图3 节点机信任模型

（1）直接信任度

对于直接信任度，本文主要考虑两个方面：节点机网络通信过程中的信息交互信任度和节点机行为信任度。信息交互信任度，是指发送交换机 i 与其交互节点机 j 在时间周期内根据直接信息交互成功次数和失败次数所计算的信任值。信息交互信任度服 *Beta* 分布。r_{ij} 表示评估节点机 i 认为被评估节点机 j 的信息交互信任值，α_{ij} 和 β_{ij} 分别表示评估节点机 i 与被评估节点机 j 过去成功交互的次数及失败交互的次数。因此，信息交互信任度可表示为：

$$r_{ij} = E\big(Beta(\alpha,\beta)\big) = E\big(f(p|\alpha,\beta)\big) = \frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \quad (1)$$

式中：

$$f(p|\alpha,\beta) = \frac{p^{\alpha-1}(1-p)^{\beta-1}}{\int_0^1 u^{\alpha-1}(1-u)^{\beta-1}du} = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \quad (2)$$

节点机行为信任度，是指在进行网络通信过程中，根据节点机是否存在异常行为来获取，主要是用来感知节点机可疑行为并及时调整节点机信任度。依据评估节点机在监控过程中被评估节点机异常行为出现的频次，计算被评估节点机行为信任度的信任值。将 b_{ij} 表示为评估节点机 i 认为的被评估节点机 j 的行为信任值，节点机行为信任度可表示为：

$$b_{ij} = \frac{b_{ij}^*}{2} \quad (3)$$

式中：b_{ij}^*为上一时间段评估节点机 i 认为的被评估节点机 j 的行为信任值。

异常端口行为检测主要针对光纤通信网络中可能存在的一些攻击行为，与物理光层中存在的安全威胁[6]不同，恶意节点机可能实施的攻击行为有以下几种。

窃听攻击[7]：当信号或数据在光网络中传递时，未经保护的信道上传输的数据就可能会遭遇外部恶意节点的截获，经过一些手段分析出数据包的部分内容进行解析，这通常是发起其他外部攻击的基础。

消息篡改攻击：外部或内部攻击者可以将截获到的消息进行修改之后再传给原定的接收者。修改内容可以是固定不变的对象，也可以是需要更新变化的对象，从而使得本身需建立的光路无法建立，将光连接请求阻断。

重放攻击：在网络通信过程中，攻击者可能会截获光包或协议消息，并在一段时间后将其重复传递给消息接收者，以此来破坏通信的完整性或实施欺骗行为。

伪造攻击[8]：攻击者可以伪造光包、ResvErr 消息、路由消息，使相应缓存区域未能按需预留波长等资源，影响光通路正常的建立和维护。

DoS 攻击[9]：这种攻击手段的实施方式非常狡猾，它利用了网络的脆弱性，通过大量的无效报文和异常操作，对光传输链路造成了严重的干扰。这种干扰不仅影响了通信的质量，还可能导致资源耗尽，进一步破坏网络的稳定性。更令人担忧的是，这种攻击的影响范围可能会随着网络结构的扩大而扩大，对整个自治域的服务质量造成严重影响。因此，需要更加警惕，采取有效的措施来防止这种攻击的发生。综上可以看出，将节点行为信任度加入到节点的直接信任度评估中是非常有必要的，节点机直接信任度的计算公式为：

$$T_{i\to j} = ar_{ij} + bb_{ij} \quad (4)$$

式中：$a\in[0,1]$ 为交互因子，表示评估节点机 i 对交换成功率的借鉴程度；$b\in[0,1]$ 为行为因子，表示评估节点机 i 对节点机行为的借鉴程度，且 $a+b=1$。

（2）间接信任度

间接信任度，是指评估节点机通过被评估节点机的其他相邻节点机反馈的对被评估节点机 j 的直接信任度，是一种对节点机进行空间维度的信任评估。它具体表现为：评估节点机 i 需要对被评估节点机 j 进行更进一步的信任度评估时，评估节点 i 向其邻居节点广播一个查询信息获取被评估节点

机 j 的推荐信息，一旦收到该查询信息，推荐节点 p 就以其对被评估节点机 j 的直接信任作为推荐信息返回给评估节点机 i。节点机 i 由推荐节点 p 反馈的被评估节点机 j 的间接信任值 $T_{i\to j}^{p}$ 可表示为：

$$T_{i\to j}^{p}=\sum_{p=1}^{n}(w_pT_{p\to j}) \tag{5}$$

式中：w_p 为各推荐节点 p 的推荐信任权重。

（3）综合信任度

假设 $x\in[0,1]$ 为直接信任因子，表示评价节点机 i 对直接信任度的借鉴程度；$y\in[0,1]$ 为间接信任因子，表示评价节点机 i 对间接信任度的借鉴程度，且 $x+y=1$。故节点机的综合信任度 $T_{i\Rightarrow j}$ 可表示为：

$$T_{i\Rightarrow j}=xT_{i\to j}+yT_{i\to j}^{p} \tag{6}$$

（4）信任度的初始化和更新

本文提出的信任模型规定，信任模型从 t_0 时刻开始运行，进入第一周期。当某节点机 A 加入 FC 网络时，为其分配初始信任度 T_A=0.5；在每个信任周期结束时，系统会进行时间间隔为 T_r 的信任度更新流程，这一过程中，所有节点机的信任度表都会根据既定规则进行调整。具体来说，对于任意节点机 A，若其在上一周期的信任度被记录为 T_{-1}，而在当前周期的信任度变为 T_0，设 A 的历史信任因子为 $y\in[0,1]$，系统将按照以下算法重新计算并调整其信任度：

$$T=\sigma\cdot T_{-1}+(1-\sigma)T_0 \tag{7}$$

如果在一个完整的信任周期内，节点机 A 既未参与任何网络数据传输，也未表现出任何异常行为，那么在更新其信任度时，系统将引入一个时间衰减因子 δ 来反映这种无活动状态对信任度的影响。通过这种方式，系统能够更准确地反映节点机在实际网络环境中的行为模式和可信度，其更新机制为：

$$T=\delta\cdot T_{-1} \tag{8}$$

为了确保 FC 网络的整体安全性和稳定性，系统会密切监视所有节点机的信任度变化。一旦某个节点机的直接信任度在更新后跌至 0.2 以下，该节点机就会被立即从网络中移除。这一措施旨在确保网络中剩余的节点机能够在一个更加可靠和安全的环境中进行光纤通信，从而有效防范潜在的安全威胁和攻击。

3 设计实现

本文设计的信任模型将应用于 FC 交换网络节点机登录后与交换机通信直至下线的整个过程，假设交换机端口均不会出现恶意行为（不存在外部攻击，也不存在内部攻击，仅作为信息数据的传递者），在节点机端加入基于信任模型的信任管理模块，从而维持整个网络的安全性及稳定性。

3.1 FC 网络软件架构

交换机端软件需要实现的模块有链路状态管理模块、FC-ELS 帧传输接收模块、FPGA 访问控制模块以及串行控制台接口。链路状态管理模块利用中断机制来探测新设备的接入情况，而 FC-ELS 帧传输接收模块则设立专门的接口以实现 FC-ELS 帧的发送与接，以此同各个节点机设备进行登录信息的交流。FPGA 访问控制模块负责获取网络地址及时间戳信息，激活端口的 FC 网络数据通信功能。至于串行控制台，则用于显示在该交换机上注册和登录的所有节点机设备信息。

节点机设备端的软件开发包含了五个模块：通信配置模块、FC-ELS 帧传输接收模块、FPGA 访问控制模块、串行控制台接口以及信任管理模块。通信配置模块会把节点机设备的网络地址信息写入到 FPGA 的存储器中；FC-ELS 帧传输接收模块用来和交换机进行登录信息交互；FPGA 访问控制模块用来获取网络地址、同步时间戳信；串口控制台可以查看交换机确认节点机登录信息；信任管理模块可以监控节点行为，将信任值低于设定阈值的节点机剔除该网络。

3.2 节点机信任管理模块

将本文提出的信任模型应用于节点机的信任管理模块 [10] 对节点进行信任评估，节点机信任管理模块如图 4 所示。每个节点都会维护三张表统称为节点行为记录表，包含直接信任表、间接信任表和历史信任表。利用光纤通信网络的广播特性，直接信任表通过主观监测其邻居节点在网络通信过程中的行为得到，间接信任表来自邻居节点 ELS 广播帧中的被评估节点的直接信任值数据，历史信任表是历史记录的节点机综合信任值，通过对邻居节点行为监测记录在节点行为记录表中，更新邻居节点的直接信任值联合间接信任值、上一阶段的历史信任值计算节点本周期的综合信任值，进而更新邻居节点的历史信任值，将本周期综合信任值小于设定阈值的节点剔除网络。

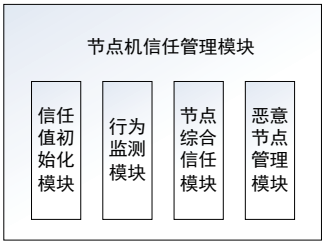

图 4 节点机信任管理模块

3.3 节点机信任评估实现

如图 5 所示，依据节点设备端软件的结构设计，其工作流程如下：当设备启动时，软件开始初始化，并将节点机初始的信任值设定为 0.5；接着，依照通信配置表设定节点机设备的网络地址；新设备上线的信息会通过中断方式传递给交换机，一旦节点机设备接收到交换机的端口登录请求帧，就会触发 ELS 发送函数回应一个端口登录确认帧给交换机；当节点机设备接收到交换机的端口登录确认帧之后，它会显示节

点设备已成功登录并开始数据通信。

本文以48端口交换机为例，假设48端口所接节点机均已上线并完成节点机信任值初始化为0.5，以将节点1设置为评估节点机，将节点2设置为被评估节点机。当节点机1和节点机2互相通信时，可通过对节点2的行为监测获取到节点2的直接信任值，并将此直接信任值填充进广播ELS数据帧中，通过交换机发送给节点2的其余所有邻居节点，节点2的其余邻居节点也会将它们对节点2的直接信任值通过广播ELS帧发送给节点1，从而节点1可计算出节点2的间接信任值，节点机1会在每周期对节点2进行一次直接信任值、间接信任值及综合信任值的计算，从而判断节点机2还是否能进行安全可靠的通信，将综合信任值低于信任阈值0.2的节点机从通信网络中剔除。

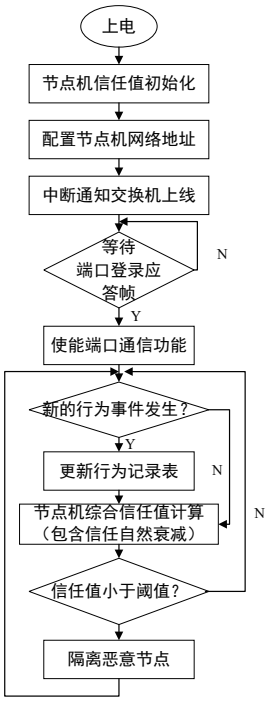

图5 节点机端处理流程

3.4 节点机信任管理模块功能测试

本文构建由一个48端口交换机和48个节点机的FC交换网络（如图1所示），节点初始化信任值为0.5，信任阈值设置为0.2，信任周期 T_r 设置为1 s。设计四组对照试验，一组在正常网络情况下，三组存在不同形式的恶意攻击行为，模拟分析不同情况下该信任模型对FC交换网络中的恶意节点识别和剔除情况。交换机域为1，节点机通信配置表中网络地址分别为0x10000、0x10001、…、0x10047，假设节点机1（网络地址为0x10000）在整个测试周期内行为正常，节点机7（网络地址为0x10006）在上线后会发起篡改攻击，更改ELS帧内数据包内容后转发给其他节点机，节点机16（网络地址为0x100015）在上线后会发起DoS攻击发布大量的连接请求抢占网络资源，节点43（网络地址为0x100042）在上线后会发起重放攻击，将截获到的数据包过1 s后重复发送给消息接收者。整个系统上电后，所有节点上线进行信任值初始化为0.5并完成登录，输出登录成功信息，节点机0x10000输出信息见图6，其他完成登录节点机输出信息相同。整个网络在经过若干个 T_r 信任周期后，可以观察到发起攻击的节点机16、43、7依次下线，节点机端口输出登录失败信息，如图7所示（将多节点串口打印信息合并）。

```
FIC 0x10000 Success
```

图6 节点机输出信息图

```
FIC 0x10015 Failed
FIC 0x10042 Failed
FIC 0x10006 Failed
```

图7 恶意节点机串口打印图

综合以上实验测试结果可以得出，本文设计的应用于FC交换网络的节点机信任管理方法能够快速准确地检测出网络中的攻击节点机，并进行有效的隔离。

4 结语

本文设计并实现了一种FC交换式网络节点机信任管理方法，设计方案包括信任模型的设计、信用模型的应用和节点机信任评估的实现。实验测试结果表明，将本文设计的信任模型应用于节点机的信任管理模块中，可以阻止发起恶意攻击的节点继续生存于整个FC网络中，可以有效识别并将其剔除网络，从而提高FC网络的安全性。

本文设计的信任模型中各信任因子所占权重只是客观选取，后续可以结合D-S证据和博弈论对各信任因子的权重进行更加理性客观的选取，提高节点机的智能决策能力，维护FC网络的公平性和公正性。

参考文献：

[1] 田泽，徐文龙，许恒，等.FC光纤通道技术研究综述[J].电子技术应用,2016,42(9):143-146.

[2] 陈龙，黄进.光网络安全及其拓扑结构隐藏方法[J].半导体光电,2006,27(6):756-759.

[3] 彭兆军.光纤传感网络入侵中未感染节点检测方法[J].科技通报,2018,34(4):154-157.

[4] 武华.FC网络配置方法[J].硅谷,2011(10):172-173.

[5] 西北工业大学.一种基于节点行为的水声传感网络节点可信度评估方法:CN202210349472.2[P].2022-06-24.

[6] 李茂田，王小双，由慧颖.光网络物理安全技术探析[J].互动软件,2021(7):2406+2408.

[7] 赵峰，邓大鹏，郭春晓，等.一种新的光信道窃听和攻击方法研究[J].光通信技术,2008,32(1):52-54.

[8] 彭伯彦.光学加密系统的攻击和防御研究[D].杭州：杭州电子科技大学,2022.

[9] 江先亮，金光，杨建刚，等.面向自治域的DoS攻击流抑制模型[J].通信学报,2013(9):134-143.

[10] 李小龙，黄廷磊，林亚平.传感器网络中一种评估节点诚实性的信任管理机制[J].计算机研究与发展，2011,48(z2):208-211.

【作者简介】

张奕然（1997—），女，湖北十堰人，硕士，助理工程师，研究方向：网络信息安全。

（收稿日期：2024-02-23）