**重庆邮电大学《计算机网络》课程报告**

**2024-2025学年第 1 学期**

**题 目 计算机网络关键技术研究**

**姓 名 邓景文**

**学 号 2022211817**

**专 业 计算机科学与技术**

**班 级 04012202**

**成 绩**

**2024年 12 月 9 日**

报告格式要求:  
1、报告题目:要求准确、简练、醒目。  
2、摘要:报告主要内容的梗概，要求简短、准确、精炼，字数限定在100-150。采用宋体小四号字体，1.5倍行距。  
3、关键词:反映报告主旨最关键的词句，要求**3-5**个，采用宋体小四号字体。

4、标题: 一级标题采用宋体三号字体，二级标题采用宋体四号字体，三级标题采用宋体小四号字体。  
5、正文:要求字数不少于**1000**字，论文正文的中文宋体小四；英文字体则要求为Times New Roman小四号，1.5倍行距。

6、参考文献的著录格式严格按照以下形式书写（含标点符号）：

（1）专著：作者. 书名. 版本(第1版不著录)[M]. 出版地: 出版者, 出版年: 起止页码.

（2）译著：作者. 书名[M]. 译者, 译. 出版地: 出版者, 出版年: 起止页码.

（3）期刊：作者. 题名[J]. 刊名, 出版年份, 卷(期): 起止页码.

（4）会议论文集：作者. 题名[C]// 编者. 论文集名. 出版地: 出版者, 出版年: 起止页码.

（5）学位论文：作者. 题名[D]. 保存地: 保存者, 年份.

（6）专利文献：专利申请者. 题名. 专利国别, 专利号[P]. 公告日期或公开日期.

（7）标准：责任者. 标准代号 标准名称[S]. 出版地: 出版者, 出版年.

（8）电子文献标注格式：主要责任者. 题名: 其它题名信息[文献类型标志/文献载体标志]. 出版地: 出版者, 出版年(更新或修改日期)[引用日期]. 获取和访问路径.

评分标准:  
1、所写技术一定要是计算机网络的关键技术; (30 分)  
2、对所描写的关键技术在网络中的作用、特点、实现及目前存在的问题等阐述深刻; (30 分，其中作用特点10分、实现10分、存在问题10分)  
3、论文条理清楚，图表齐全，格式规范; (20 分)  
4、论文所写关键技术是经过整理，自己理解后的观点; (10 分)

5、能对所阐述的关键技术加入自己的分析总结; (10 分)

# 计算机网络关键技术研究

**摘 要：**本文讨论了计算机网络两大支柱技术：数据加密与路由技术。数据加密技术通过多元加密策略，筑起网络安全防线，有效应对各种安全挑战。路由技术确保信息精准送达，提升网络灵活性并优化服务品质。本文主要分析了它们的运作原理及存在的问题。

**关键词：**计算机网络，数据加密技术，路由技术

## 1引言

计算机已成为生活与工作的核心工具，然而计算机网络在提供便利的同时，也面临很多的信息安全挑战。为了应对这些挑战，产生了数据加密技术，主要是为了提升网络信息的安全性。路由技术是网络通信的基石，确保数据的高效、实时传输。

本报告综合两篇论文（《数据加密技术在计算机网络信息安全中的应用探讨》，《计算机网络通信中的路由技术》），理解了数据加密技术在保障计算机网络信息安全中的应用，以及路由技术在促进网络通信效率方面的作用。

## 2数据加密技术

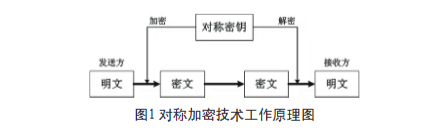
### 2.1计算机网络信息安全主要威胁类型

计算机操作系统存在安全漏洞：操作系统是计算机正常运行的基石，但系统漏洞容易被黑客和木马病毒利用，从而对计算机进行远程操控，严重威胁信息安全。

计算机数据库系统管理存在安全漏洞：数据库系统在数据管理与处理上存在差异，现有数据加密技术难以完全满足数据库系统的安全需求，导致管理上存在漏洞。

### 2.2数据加密技术主要形式

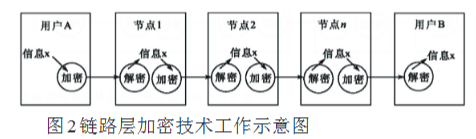
对称加密技术：加密与解密过程中使用的密钥一致，具有加密解密效率高的优势，适用于海量数据的加密解密工作。然而，密钥的保管成为关键，一旦泄露，信息安全将无法得到保障。



非对称加密技术：加密与解密过程中使用的密钥不一致，具有公开密钥和私有密钥两种。私有密钥才能实现文件的解密，提高了数据信息的安全性。但总体计算量庞大，消耗时间较多，主要应用在少部分数据加密工作中。

### 2.3数据加密技术在计算机网络信息安全中的具体应用

链路层加密技术：通过链路层加密，传输中的所有数据的各个节点都需要执行数据解密和再加密工作，直至所有数据信息全部传输完成。很好保证了数据传输的安全性，但存在同步性问题、节点物理层安全性问题以及密钥管理问题等。



端对端加密技术：消息在发出之前进行加密处理，直到消息在被接收以后才进行解密。在传输过程中始终处于加密状态，简化了设备，解决了数据传输同步性问题。但信息的起始点与结束点明显，降低了数据传输的安全性。

数字签名和报文分辨技术：通过数字签名和报文分辨技术，可以识别出信息的真实性与完整性，有效应对信息更改、信息伪造等问题。

## 3计算机网络通信中的路由技术

### 3.1路由技术的应用特点

技术应用重要性：路由技术在多个网络或网段中起到重要连接作用，是网络通信的重要环节。

加强信息完整性：路由技术不仅能完成数据信息的实时传递，还能在传递过程中对数据信息进行有效修正并实时跟踪。

提升网络环境的灵活性：利用安全过滤机制对网络通信进行管理控制，提升网络环境的安全性及信息传递速度。

优化网络服务品质：交换型路由器通过优先排序功能，适当调整网络流量并进行数据节能型分析，选择最佳路线。

### 3.2路由交换技术的主要理论基础

路由技术：路由器接收数据包并进行解析，通过路由表查找信息数据传输目标，确定转发目标后进行打包整理。

主流路由器协议技术：包括高级口令认证路由器协议和口令认证，其中高级口令认证录取协议的安全性更高。

路由算法：常见的计算方法包括距离矢量路由算法和链路状态路由算法，用于判断最佳路径。

路由协议：互联网在运行过程中，需要使用链路状态路由算法和距离矢量路由算法计算路径，通过分化方式形成若干个自制系统（AS）完成传播路径的选择。

### 3.3交式路由器和传统交换机的差异

传统交换机与路由器运用：普通交换机主要使用数据链路层，路由器在网络层发挥作用。

第三层交换和路由交换机：第三层交换利用线速交换技术提升速度，具有良好的稳定性及低功耗优势。

|  |  |  |
| --- | --- | --- |
| **比较基础** | **路由器** | **Switch 开关** |
| Opera层 | 路由器在 OSI 模型的第 3 层（网络）运行。 | 网络交换机运行在第二层（数据链路层） OSI模型. |
| 提供的服务 | 路由器将提供 NAT、NetFlow 和 QoS 服务 | Switch 不会提供此类服务。 |
| 地址维护 | 将IP地址存储在路由表中，并自行维护一个地址。 | 将 MAC 地址存储在查找表中并自行维护地址。但是，交换机可以学习 MAC 地址。 |
| 端口 | 网络设备 2/4/8 端口。 | 交换机是一种多端口网桥。24/48 个端口。 |
| 模式 Transmission | Less Duplex | 在全双工下，不会发生冲突。 |
| 速度极限 | 无线连接的速度限制为 1-10 Mbps，有线连接的速度限制为 100 Mbps。 | 交换机的速度限制为10/100Mbps。 |
| 路由决定 | 帮助用户更快地做出路线决策 | 可能会做出更复杂的路线决策 |
| NAT | 路由器可以执行 NAT | 交换机无法执行 NAT |
| 用法 | 在各种类型的网络环境（MAN/WAN）中，路由器比交换机的运行速度更快。 | 在局域网环境中，交换机比路由器更快。 |
| 广播域 | 在路由器中，每个端口都有自己的广播域。 | 该交换机除了实现的VLAN外，还有一个广播域。 |
| 地址类型 | 路由器操作围绕 IP 地址进行。 | 开关适用于 MAC地址 因为它在单一网络范围内运行。 |
| 连接线路 | 路由器可以在有线和无线网络环境中工作。 | 交换机仅限于有线网络连接 |

### 3.4 计算机网络路由交换技术的下一步发展趋势

路由器和交换机的配置统一：路由器与交换机的相关配置结合统一，成为技术未来发展方向之一。

与IP子网提升结合程度：定制更加科学的配置方案进行管理，活跃IP子网的连通性。

重视路由器协议的管理问题：提升数据资料的及时更新效果，防止误会，提升网络环境的安全性。

## 4存在的问题

### 4.1数据加密技术

对称加密技术的密钥管理困难，一旦密钥被窃取，信息安全性无法保证。

非对称加密技术计算量庞大，消耗时间较多，影响加密效率。

链路层加密技术存在同步性、节点物理层安全性和密钥管理等问题。

端对端加密技术不隐藏信息地址，降低了数据传输的安全性。

### 4.2路由技术

传统路由器在处理数据过剩或浮动时可能受到影响。

路由协议在计算路径时可能占用宽带资源。

路由器的相关协议管理需要专业人员进行操作，对人员素质要求较高。

## 5总结

数据加密技术和路由技术是计算机网络通信中的两大核心领域，它们共同支撑现代计算机网络的安全、高效运行。数据加密技术通过保护数据的机密性、完整性和真实性，为网络通信提供了基本的安全保障；路由技术通过选择最佳传输路径和优化网络通信过程，确保了数据的快速、准确传输。两者共同推动了计算机网络通信技术的发展和进步。

随着云计算、大数据、物联网等新技术的不断发展，计算机网络通信将面临很多的安全挑战。因此，数据加密技术和路由技术也需要不断创新和发展，以适应新的网络安全需求。

关于数据加密技术，未来可以探索更加高效、安全的加密算法和协议，以提升数据加密的效率和安全性；也可以研究更加智能的密钥管理和分发机制，降低密钥泄露的风险；还可以结合人工智能、机器学习等新技术，实现数据加密技术的自动化和智能化，提高网络安全的整体水平。

路由技术方面，未来可以进一步优化路由算法和协议，提高网络通信的效率和稳定性。也可以加强路由技术的安全性研究，防止路由攻击和网络拥塞等问题的发生。还可以结合新型网络技术，如软件定义网络（SDN）、网络功能虚拟化（NFV）等，实现路由技术的灵活部署和动态优化，提升网络通信的智能化和自适应能力。

数据加密技术和路由技术是计算机网络通信中的两大重要领域，它们的发展和创新将不断推动计算机网络通信技术的进步和升级。我们需要持续关注这些领域的研究和发展动态，积极探索新的技术和方法，构建更加安全、高效、智能的计算机网络通信系统。

### 参考文献

1. 李正伟, 周锐. 数据加密技术在计算机网络信息安全中的应用探讨[J]. 数字通信世界, 2021(06): 198-199。
2. 王思宇. 计算机网络通信中的路由技术[J]. 新型工业化, 2022, 12(02): 29-31.
3. 路由器与交换机 —— 两者的区别 [EB/OL]. 2024 [2024-12-18]. <https://www.guru99.com/zh-CN/router-vs-switch-difference.html>.