基于改进 DES 算法的网络链路安全通信方法

吴静莉
(鹤壁职业技术学院 电子信息工程学院,河南 鹤壁 458030)

摘要:现有的安全通信方法受限于 60000 kB 数据量,存在摘要对等数目不稳定的问题。为此,文章提出基于改进 DES 算法的网络链路安全通信方法。该方法通过网络链路安全协议建立连接,验证双方身份;利用最短路径优先协议,结合数据库信息,确保可信连接适应网络环境;基于密文位数,使用 DES 算法延长密钥,使之与明文位数匹配;设置访问权限,运用双线性映射配对特定属性,并通过加密算法处理,实现安全通信。实验证明,传输数据量稳定在 90000 kB,提升了效率,解决了摘要对等数目不稳定的问题,提高了通信性能。

关键词:DES 算法;网络链路;安全通信;改进算法
中图分类号:TP399 **文献标志码**:A

0 引言

随着现代技术的发展,网络链路安全通信面临着诸多挑战。在当前通信环境中,利用互联网技术调整发射端信号定点,可确保信号能准确到达合法接收端,保障通信安全。如卢为党等[1]利用无人机扩展通信范围,结合智能路由算法优化数据传输路径,以减少传输时延。但无人机中继系统容易遭受外部干扰攻击,导致通信被截获。李子能等[2]运用智能反射面调整信号传播环境,结合协作干扰策略对抗恶意攻击,实现无人机安全通信。但如果智能反射面控制算法存在漏洞会被攻击者利用,进而会对通信进行篡改或破坏。因此,本文研究基于改进 DES 算法的网络链路安全通信方法,对提升网络链路的安全通信能力有重要意义。

1 网络链路安全通信方法

1.1 建立安全连接

本文使用网络链路安全协议,通过密钥交换技术来建立安全连接,即使用公钥基础设施和密钥分发中心来安全地分发和管理密钥。首先,双方通过公钥交换或预共享的密钥进行身份验证,并协商出一个会话密钥。这个会话密钥将用于后续的通信加密和解密。通过使用私钥进行加密和公钥进行解密(或相反),确保通信的机密性,即只有拥有正确密钥的双方才能理解和修改传输的数据。在本文提出的方法中,当网络中的节点(假设节点数量为 n 个)尝试建立连接时,不仅要确保信息传输的完整性,还要确保连接的可靠性和安全性。为了实现这一目标,本文采用端到端的路径策略,确保数据在传输过程中不会被中间节点篡改或窃取。在可信连接的建立过程中,引入最短路径优先协议,利用链路状态数据库来确定网络中的拓扑结构。通过最短路径优先协议,可以计算出从源节点到目标节点的最短路径,并基于这条路径建立连接。根据数据库中的信息计算满足特定的可信度。设定 e 来表示节点之间的可信度,则可信连接度的公式为:

$$e = w_1 \sum^{i=d} \frac{1}{h} + w_2 \sum^{i=d} \frac{1}{h} + w_3 \sum^{i=d} \frac{1}{h} \tag{1}$$

式中,h 为节点链路带宽;d 为源节点;w 为权重。根据可信度计算结果形成路由表。

1.2 改进 DES 算法密钥延长

首先,改进 DES 算法在开始加密之前,对输入的待加密数据进行预处理。数据被精确地分割为多个 64 bit 块,这是 DES 算法的标准操作块大小。如果待加密的数据长度不是 64 位的整数倍,算法会按照特定的规则在数据的末尾添加额外的位以补齐最近的 64 位边界。其次,算法会按照 DES 的初始置换规则对每一个 64 位的数据块进行置换,旨在打乱数据的原始位序,增加密码分析的难度。在置换之后,算法会进一步打乱明文的序列,以增强加密过程的安全性。最后,这 64 位的数据会被均匀地分为 2 个 32 位的分组。这 2 个分组将分别进行后续的加密操作。

在密钥生成阶段,算法会要求用户设置一个初始的 64 位密钥 k。然而,与原始 DES 算法不同,改进版本通过压缩算法将初始的 64 位密钥转化为 54 位的有效输入密钥。得到的 54 位有效密钥会被进一步分

作者简介:吴静莉(1980—),女,讲师,硕士;研究方向:软件技术。

为 2 部分,分别用于不同的加密阶段或操作。为了增加密钥的复杂性和安全性,改进 DES 算法引入了密钥的循环移位机制。在每一轮加密过程中,密钥都会进行循环移位操作。移位的次数和模式是由算法精确控制的,可以根据需要进行调整。每次移位后的密钥都会作为下一轮加密的输入,同一个初始密钥在加密过程中会产生多个不同的密钥变体。

在每个轮次结束时,2 部分密钥会被合并起来,形成一个新的有效密钥。这个新密钥将用于下一轮的加密操作。通过这种方式,密钥的长度在加密过程中得到了有效的延长,从而提高了算法的安全性。整个加密过程会包含多个轮次(通常为 16 轮),每个轮次都会使用更新后的密钥对明文分组进行加密操作。在每个轮次中,算法会使用不同的函数和运算来混淆和扩散明文数据,以产生难以预测的密文输出。

当所有的加密轮次都完成后,最终产生的密文会按照规定的逆置换规则进行置换,以恢复其原始的位序。最终,这个经过精准加密的密文可以被安全地存储或传输到目标位置。在解密过程中,接收者会使用相同的密钥和算法来恢复原始的明文数据,确保数据的完整性和安全性。循环移位过程须满足特定条件:

$$\begin{cases} c = Ls(c-1) \\ d = Ls(d-1) \end{cases} \tag{2}$$

式中,Ls 为循环变换过程;c 为左循环;d 为右循环。在对子密钥进行压缩置换时,每个子密钥中的第 8 位数据会丢失,子密钥的长度缩短为 46 位[3]。对明文进行逆置换操作,输出置换结果,得到最终密文。根据密文位数用 DES 算法延长密钥,确保与明文位数匹配。加密解密过程有明确的数学描述:

$$\begin{cases} DES^{-1}(DES_k(x)) = x \\ DES(DES_k(x)) = x \end{cases} \tag{3}$$

式中,k 为初始密钥,使用第一组密钥进行解密操作。为增强混淆效果,使用第一组密钥组加密,再用下一组密钥解密,最后以第一组余下的子密钥完成加密。此方式可使密钥量翻倍,提高位数阶数。解密时,须输入第三组子密钥,再输入下一组,最后输入第一组,顺序与加密相反。

1.3 信息传输安全通信

为实现信息安全传输,本文通过结合密钥的方式对网络链路信息进行安全通信。通过实施身份验证机制,例如使用公钥基础设施进行数字证书验证,可以有效地确认发送方和接收方的真实身份,从而大大降低冒充行为。当通信过程涉及访问权限管理时,为了更精准地控制资源的访问,本文采用双线性映射技术对特定属性进行配对,将用户的身份、角色或其他关键属性与所需访问的资源进行精确匹配,从而实现更加细化和灵活的访问控制策略。由于通信过程涉及访问权限管理,因此,本文运用双线性映射技术对特定属性配对[4],公式为:

$$u(a\cdot q, b\cdot z) = p(b\cdot q, a\cdot z) \tag{4}$$

式中,a、b 为给定整数;q、z 为样本。通过配对访问控制,限制特定用户或系统访问网络资源,保障网络链路通信安全[5]。利用协商好的安全信道密钥加密解密信息,实现保密传输。附加安全标签于 IP 信息尾部,包括明文字段(链路层协议头、主要信息)和密文字段的安全标签,确保信息完整传输[6]。末尾字段为安全标签,由链路安全密钥转换生成,标签为:

$$kj = kG \tag{5}$$

式中,G 为有限域。通过获取最新的安全标签,对端网络安全终端会执行验证,以确保 IP 信息是由认证终端发送且未被篡改。安全标签作为身份验证的重要标识,能够确保数据的完整性和真实性。通过为数据或系统组件附加特定的安全标签,能够快速、准确地识别任何未经授权的修改或篡改[7]。

2 实验测试与分析

2.1 搭建实验环境

实验在 MATLAB 下分析差分跳频通信认证,采用 50000 样本,跳频 3200 跳/s,频段 3.24~4.41 MHz。Turbo 编码,信噪比 12.5~15.5 dB。数据存储在数据库中,设备为 i7 CPU、128 G 内存、Windows 11。数据采集使用操作主机及 Ubuntu8 虚拟机。实验设置实验组和对照组,以测试本文方法提升传输数据量的效果。

2.2 结果与分析

在设置好的实验中,对样本数据集进行整理,对通信效果进行测试。在相同的样本下,对测试样本进行分类与提取,获得不同小组的传输数据量结果,如图 1 所示。

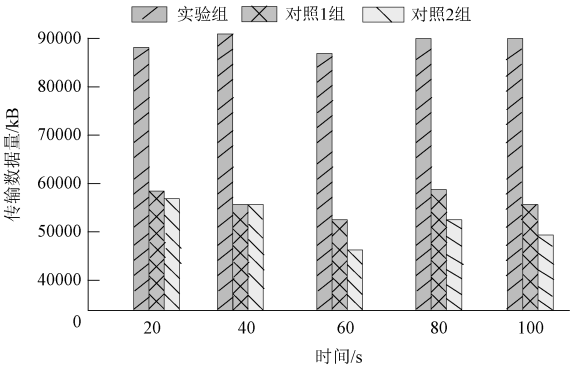

图 1 传输数据量结果

由图 1 可知,实验组传输数据量稳定在 90000 kB 左右,显著高于对照组的 60000 kB 以下,证明改进 DES 算法提升了数据传输效率,同时确保了安全性并能够抵御网络攻击和数据泄露风险,在大数据和复杂网络环境中具有优势。在 MATLAB 仿真下,10 次测试信息数据摘要对等数目稳定在 80~81 个,证明该方法有效,实现成功认证。

3 结语

本文提出的基于改进 DES 算法的网络链路安全通信方法,解决了数据加密问题,确保了网络通信中信息的完整性。然而,该方法仍存在不足。未来,笔者将继续完善算法计算,将改进的算法应用于网络链路安全通信,结合其他安全机制,实现良好的应用效果。

参考文献

[1]卢为党,曹明锋,高原,等. 基于智能反射面辅助的无人机中继系统安全通信方法[J]. 电子与信息学报,2022(7):2273-2280.
[2]李子能,胡智群,肖海林,等. 智能反射面和协作干扰的无人机安全通信算法[J]. 北京邮电大学学报,2023(1):69-76.
[3]林敏,张健,林志,等. 多播传输模式下的卫星通信安全波束成形算法[J]. 电子学报,2022(1):98-105.
[4]李萌,孙艺夫,安康,等. 非理想信道状态信息下 RIS 辅助的安全通信[J]. 电讯技术,2023(7):1017-1027.
[5]刘文涛,AHMED M,林青. 基于 DRL 的主动 RIS 安全无线通信优化方法[J]. 计算机应用研究,2023(9):2808-2814.
[6]谢鑫,单崇喆,吴云峰,等. 三维方向调制的弹载遥测安全通信方法[J]. 探测与控制学报,2022(6):58-62.
[7]高建邦,高国旺. 一种智能超表面辅助的非视距安全通信方法[J]. 西安电子科技大学学报,2023(2):64-70.

(编辑　王雪芬)

Secure communication method for network links based on an improved DES algorithm

WU Jingli
(Electronic Informational Engineering College, HEBI Polytechnic, Hebi 458030, China)

Abstract: The existing secure communication methods are limited by 60000 kB of data and have the problem that the number of abstract peers is unstable. Therefore, this paper proposes a network link security communication method based on improved DES algorithm. The connection is established through the network link security protocol to verify the identities of both parties. Using the shortest path first protocol, combined with database information, to ensure that trusted connections adapt to the network environment. Based on the ciphertext bits, the DES algorithm is used to extend the key and make it match the plaintext bits. Set access rights, use bilinear mapping to pair specific attributes, and use encryption algorithms to process, to achieve secure communication. The experimental results show that the data volume is stable at 90000 kB, which improves the efficiency. Solve the problem of the unstable number of abstract peers and improve the communication performance.

Key words: DES algorithm; network link; secure communication; improved algorithm