基于信任计算的无线通信网络数据传输加密机制研究

张江鹏 [1]
ZHANG Jiangpeng

摘 要 为提高无线通信网络数据加密安全传输效果，提出基于信任计算法的无线通信网络数据传输加密方法。首先针对 AES 算法中原密钥扩展进行分析，得出其 AES 算法原密钥扩展的缺点，进行针对性的 AES 算法改进。然后，基于上述分析结果，结合信任计算从减弱密钥字之间的相关性和保留 AES 算法即时性入手，实现改进 AES 算法。最后，采用信任计算结果从加密和解码两个过程，完成对无线通信网络数据传输加密机制设置。结果表示，采用所提方法进行无线通信网络数据传输的加密，其泄漏概率较低，始终维持在 3% 以下，由此说明所提方法具有一定有效性。

关键词 信任计算；原密钥扩展；无线通信网络；数据加密；安全传输

doi：10.3969/j.issn.1672-9528.2024.02.035

0 引言

随着信息技术的迅猛发展，人们越来越多地依赖于网络进行通信和数据传输。在这个数字化时代，保护无线通信网络数据传输的安全性变得至关重要。大规模互联网的应用、普及，如电子商务、在线支付和云计算等，加密安全传输成为保护用户隐私和企业机密信息的必要手段。而信息泄露和黑客攻击等安全威胁不断增加，传统的通信方式已经不能满足安全传输的需求。为了保护无线通信网络数据传输时的机密性和完整性，通信安全领域涌现出许多加密技术和安全传输方法。这些方法通过对数据进行加密和解密，确保只有合法的接收者才能解读并使用无线通信网络数据 [1]。无线通信网络数据传输加密方法的研究旨在提供安全、可靠的方式来保护通信内容，防止未经授权的访问和篡改。此外，国家安全、商业竞争和个人隐私等因素也促使了对无线通信网络数据传输加密方法研究的关注。因此，相关领域研究学者对此展开了相应研究，牛耕 [2] 提出基于对称加密的通信网络数据多信道安全传输方法，首先建立信道链路层分布结构模型，采用分段线性组合解码进行均衡控制，然后通过随机码幅度调制方法处理传输过程中的调制解调，最后采用对称加密算法来设计密钥，完成数据加密，实现通信网络数据多信道安全传输。该方法具有较高的加密速度和效率，但它们的加密强度相对较低，容易被暴力破解或攻击，导致采用该方法进行无线通信网络数据传输加密时不够可靠。

因此，为有效提高无线通信网络数据传输加密的可靠性，提出基于新人计算的无线通信网络数据传输加密方法，以降低泄漏概率、提高破译比特长度，不断提高无线通信的安全性，保护用户的隐私和敏感信息，进一步推动信息社会的可持续发展。

1 原密钥扩展分析

AES 是一种对称加密算法，广泛用于数据保护和安全通信领域。它使用相同的密钥进行加密和解密操作，具有高度安全性和效率。密钥扩展算法是一种用于生成 AES 加密算法所需的轮密钥的算法。在 AES 中，原始密钥经过密钥扩展算法产生一系列轮密钥，这些轮密钥用于加密和解密数据。密钥扩展算法是 AES 算法的关键组成部分，用于增强安全性 [3-4]。

原本的密钥扩展过程如图 1 所示，i 表示密钥扩展的轮数，$1 \le i \le 0$。左边部分是轮密钥四个字的生成过程，上一排是上一轮密钥的四个字，下一排是生成的新密钥的四个字，每一轮密钥都是基于上一轮密钥扩展得到。右边部分虚线框里面的是 T 函数。初始密钥 K_0 加上 10 个扩展轮密钥 $K_0 \sim K_{10}$，一共 44 个字，表示为 $W[0, 43]$。

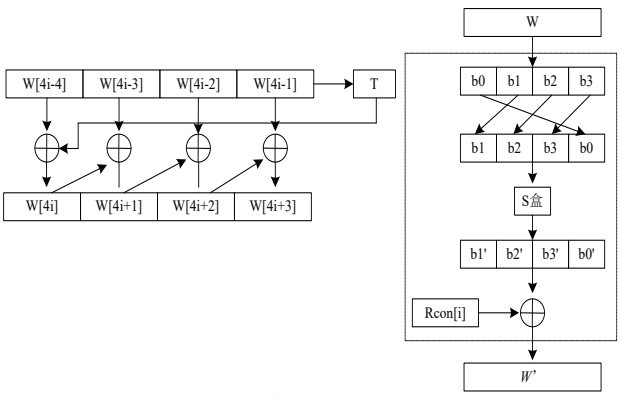


图 1 原密钥扩展原理图

1. 甘肃同兴智能科技发展有限责任公司 甘肃兰州 730050

分析原始的密钥扩展过程可知：根据初始密钥 K_0 的 $W[0]$ 和 $W[3]$ 可以得到第 1 轮密钥 K_1 的 $W[4]$，根据 K_0 的 $W[1]$ 和 K_1 的 $W[4]$ 可以得到 K_1 的 $W[5]$，根据 K_0 的 $W[2]$ 和 K_1 的 $W[5]$ 可以得到 K_1 的 $W[6]$，根据 K_0 的 $W[3]$ 和 K_1 的 $W[6]$ 可以得到 K_1 的 $W[7]$。至此，第 1 轮密钥 K_1 的四个字 $W[4]$、$W[5]$、$W[6]$、$W[7]$ 成功生成，后续轮密钥 $K_2 \sim K_{10}$ 以此类推即可全部得到。

如果攻击者得到了第 5 轮密钥 $W[20, 23]$，则可以根据第 5 轮密钥的 $W[20]$ 和 $W[23]$ 得到第 6 轮密钥的 $W[24]$，根据第 5 轮密钥的 $W[21]$ 和第 6 轮密钥的 $W[24]$ 得到第 6 轮密钥的 $W[25]$，根据第 5 轮的 $W[22]$ 和第 6 轮密钥的 $W[25]$ 得到第 6 轮密钥的 $W[26]$，根据第 5 轮密钥的 $W[23]$ 和第 6 轮密钥的 $W[26]$ 得到第 6 轮密钥的 $W[27]$。至此，就得到了后一轮密钥。

攻击者再根据第 5 轮密钥的 $W[20]$ 和 $W[21]$ 可以得到第 4 轮密钥的 $W[17]$，根据第 5 轮密钥的 $W[21]$ 和 $W[22]$ 可以得到第 4 轮密钥的 $W[18]$，根据第 5 轮密钥的 $W[22]$ 和 $W[23]$ 可以得到第 4 轮密钥的 $W[19]$，根据第 5 轮密钥的 $W[20]$ 和第 4 轮的 $W[19]$ 可以得到第 4 轮密钥的 $W[16]$。至此，就得到了前一轮密钥。以此类推，攻击者最终可以破解出初始密钥 K_0 和 10 轮密钥 $K_1 \sim K_{10}$，即获得 44 个字的全部密钥 $W[0, 43]$，进而攻破密码，威胁信息安全。

很明显，原密钥扩展算法简单高效的同时，也存在着一个致命的缺点，那就是 44 字密钥的密钥字之间存在极强的“相关性”。虽然为了增加算法的复杂性，每一轮密钥的第一个字会涉及 T 函数操作，但是该操作仍然没有从本质上改变密钥字之间关联性太强的原始性质。攻击者利用两个相关密钥字可以推出与它们强相关的第三个密钥字。也就是说，当攻击者获取到 $K_0 \sim K_{10}$ 其中任意一轮密钥 K_i，可以穷举测试 2^{32} 次推导出它的下一轮密钥 K_{i+1}，也可以继续暴力穷举搜索 2^{32} 次逆向推出其上一轮密钥 K_{i-1}。因此，对密钥扩展算法的改进迫在眉睫。

2 无线通信网络数据传输加密的实现

2.1 密钥的生成

综合以上两个考虑，改进的密钥扩展算法由两部分组成。第 1 轮密钥 K_1 的生成为第一部分 Part1，第 2 轮密钥 K_2 到最后一轮密钥 K_{10} 的生成为第二部分 Part2。

Part1：如图 2 所示，其中初始密钥 K_0 的四个字 $W[0]$、$W[1]$、$W[2]$、$W[3]$ 由随机生成器得到。第 1 轮密钥 K_1 的第一个字 $W[4]$ 和原密钥扩展算法一致，由初始密钥 K_0 的第一个字 $W[0]$ 和经过 T 函数变换以后的第四个字 $W[3]$ 异或得到。K_1 的第二个字 $W[5]$ 由该轮密钥的前一个字 $W[4]$ 进行字节代换得到，K_1 的第三个字 $W[6]$ 由该轮密钥的前两个字 $W[4]$ 和 $W[5]$ 直接异或得到，K_1 的第四个字 $W[7]$ 由该轮密钥的前一个字 $W[6]$ 进行字节代换得到。至此，第一轮密钥 K_1 的四个字 $W[4]$、$W[5]$、$W[6]$、$W[7]$ 扩展完毕。

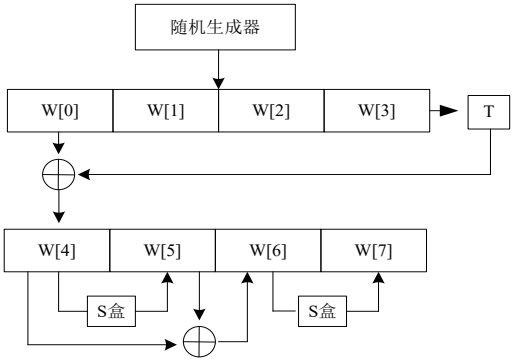


图 2 改进密钥扩展算法 K_0 和 K_1 的生成

图 2 中第 1 轮密钥 K_1 的四个字 $W[4]$、$W[5]$、$W[6]$、$W[7]$ 生成如式（1）所示，T 函数如（2）所示。

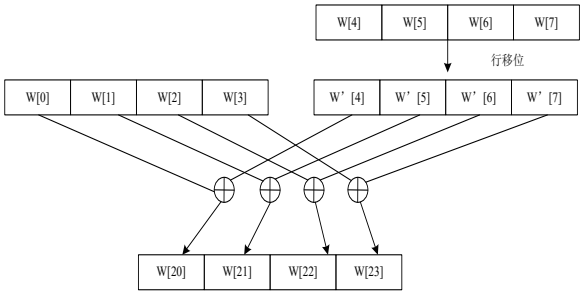
$$W[i]=\begin{cases} W[i-4]\oplus W[i-1], i=4 \\ SubBytes(W[i-1]), i=5\text{或}i=7 \\ W[i-1]\oplus W[i-2], i=6 \end{cases} \quad (1)$$

$$T(W[i-1])=SubWord(RotWord(W[i-1]))\oplus Rcon[j] \quad (2)$$

式中：*RotWord* 表示字循环，*SubWord* 表示字代换，j 表示密钥扩展的轮数。

Part2：如图 3 所示，第 2 轮密钥 K_2 的四个字 $W[8]$、$W[9]$、$W[10]$、$W[11]$ 由前两轮密钥（初始密钥 K_0 和第一轮密钥 K_1）共同操作得到。首先对第 2 轮密钥 K_2 的前一轮密钥 K_1 进行轮函数里面的行移位操作得到 K_1'，然后由 K_0 的第一个字 $W[0]$ 和 K_1' 的第一个字 $W'[4]$ 直接异或得到 K_2 的第一个字 $W[8]$，由 K_0 的第二个字 $W[1]$ 和的 K_1' 的第二个字 $W[5]$ 直接异或得到 K_2 的第二个字 $W[9]$，由 K_0 的第三个字 $W[2]$ 和 K_1' 的第三个字 $W[6]$ 直接异或得到 K_2 的第三个字 $W[10]$，由 K_0 的第四个字 $W[3]$ 和 K_1' 的第四个字 $W[7]$ 直接异或得到 2K 的第四个字 $W[11]$。至此，第 2 轮密钥 K_2 扩展完毕。

同理，第 3 轮密钥 K_3 的四个字 $W[12]$、$W[13]$、$W[14]$、$W[15]$ 由前两轮密钥（K_1 和 K_2）共同操作得到。以此类推，第 10 轮密钥 K_{10} 和 K_2 的四个字 $W[40]$、$W[41]$、$W[42]$、$W[43]$ 由前两轮密钥（K_8 和 K_9）共同操作得到。



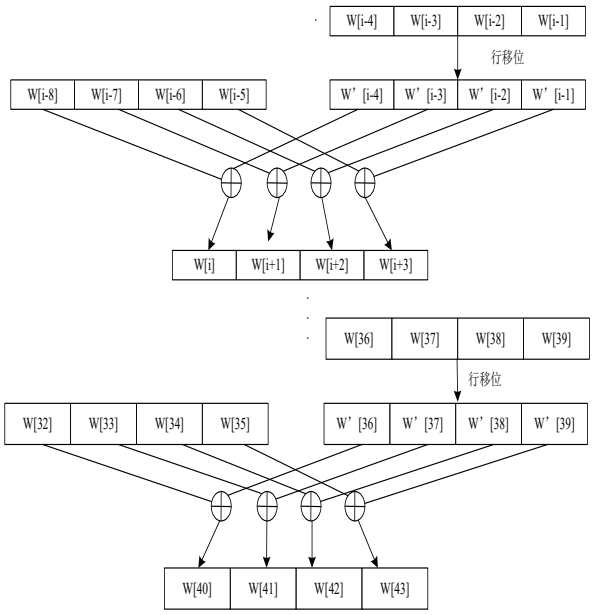


图 3 改进密钥扩展算法的 $K_2 \sim K_{10}$ 扩展过程

图 3 中，$K_2 \sim K_{10}$ 中每一轮密钥对应四个字的生成公式如（3）所示，$8 \le i \le 43$：

$$W[i]=W'[i-4]\oplus W[i-8] \tag{3}$$

式中：$W'[i\text{-}4]$ 如（4）所示，$8 \le i \le 43$：

$$W'[i-4]=ShiftRows(W[i-4]) \tag{4}$$

综上所述，初始密钥 K_0 由随机生成器得到，10 轮密钥的生成为：

$$W[i]=\begin{cases} W[i-4]\oplus T(W[i-1]), i=4 \\ SubBytes(W[i-1]), i=5或i=7 \\ W[i-1]\oplus W[i-2], i=6 \\ ShiftRows(W[i-4])\oplus W[i-8], 8 \le i \le 43 \end{cases} \tag{5}$$

2.2 信任计算的无线通信网络数据传输加密

无线通信网络是动态、实时的，用户行为也是变化的，两个节点长时间没有交互，即使早期的信任值高，现在由于不能确信交互节点是否依然表现良好，对其信任值应该有所降低，所以，信任应该具有随着时间的增长而衰减的特性。

假设到时刻 t 为止已发生的交易次数为 $N(t)$，则 t 和 $N(t)$ 间关系如图 4 所示。

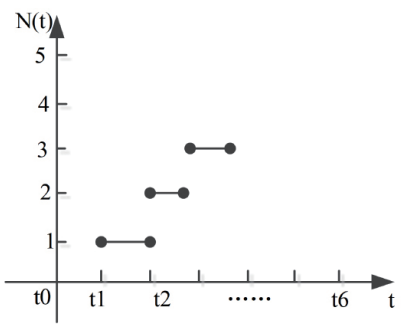


图 4 传输次数和时刻关系图

由图 4 可知，若节点在时间段 $[t_0, t_i)$ 内进行了 k 次传输，且 $\{N(t_0, t_i)=k\}$ 是一个时间，则其概率可以记为 $P_k(t_0,t_i)=P\{N(t_0,t_i)=k\}, k=1,2,...$

易得该节点在 $[t_0, t_i)$ 的时间段内传输次数和时间之间的关系满足独立增量泊松分布的三个条件，故有：

$$f(N(t))=P\{N(t+s)-N(s)=k\}=e^{-\lambda t}\frac{(\lambda t)^k}{k}, k=1,2,... \tag{6}$$

式中：K 表示传输次数，λ 为单位时间内传输次数。由此在 t 时刻需求节点 x 对服务 提供节点 y 的直接信任度为：

$$DT(x,y)=e^{-\lambda t}\frac{(\lambda t)^k}{k}DT(x_1,y_1) \tag{7}$$

两节点之间的信任在交互之后应该是会变化的，即如果两者之间交互良好，信任值会升高，两者之间的交互存在恶意行为，信任值会降低。所以，交互过后需求节点需要给予推荐节点相应的反馈信任，以此更新原有信任。在进行信任更新时，若两节点之前并没有发生过交互，则节点需求节点反馈的信任值即为两者之间的直接信任；若两节点之前发生过交互，则结合原有的直接信任状况更新现有信任值，此时仍然需要分为两种情况。

（1）安全节点直接推荐

假设节点 x 对 y 的担保评价 $FT(x, y)$，则 x 对 y 的直接信任更新为：

$$DT(x,y)_n=\omega DT(x,y)_{n-1}+(1-\omega)FT(x,y) \tag{8}$$

（2）可疑节点担保推荐

假设节点 x 对 y 的担保评价 $FT(x, y)$，对 K 的推荐评价为 $FT(x, k)$，则 x 对 y，以及 x 对 k 的直接信任分别更新为：

$$DT(x,y)_n=\omega_1 DT(x,y)_{n-1}+(1-\omega_1)FT(x,y) \tag{9}$$

$$DT(x,k)_n=\omega_2 DT(x,k)_{n-1}+(1-\omega_2)FT(x,k) \tag{10}$$

式中：ω_1、ω_2 为反馈调节参数，$DT(x, y)_n$、$DT(x, k)_n$ 分别表示节点 x 对 y、节点 x 对 k 更新后的信任值，$DT(x, y)_{n-1}$ 表示节点 x 对 y 更新之前的信任值。

考虑到目前的无线通信网络用户数量巨大，频繁进行组别的更新是不现实的，也是没有必要的，所以对于节点分组的更新，规定在新增交互次数达到原来的一定比例时，给予重新分组，具体的比例需要可以根据不同系统进行调整。

综上所述，采用改进的密钥扩展算法来实现 AES 的改进，产生一系列轮密钥，以用于加密和解密数据，并结合信任计算调整结果，完成无线通信网络数据传输加密。基于信任计算的无线通信网络数据传输加密和解密过程如下文所示。

（1）加密过程

a. 密钥生成：通信双方需要共享一个密钥，这个密钥必须是足够长且随机的字符串。

b. 数据分组：将待加密的信息分成固定长度（通常为 128 位）的数据块。

c. 初始轮密钥加：将每个数据块与初始轮密钥进行异或操作。

d. 轮函数：经过多轮（通常为10轮、12轮或14轮）的替代、置换和线性变换操作。

e. 轮密钥加：每一轮结束后，将轮密钥与数据块进行异或操作。

f. 输出：输出加密后的数据块。

（2）解密过程

a. 数据分组：将收到的加密数据按照指定的块大小（通常为 128 位）进行划分。

b. 初始轮密钥异或：将每个数据块与解密过程中对应的初始轮密钥进行异或操作。

c. 逆向轮函数：进行多轮（通常为 10 轮、12 轮或 14 轮）的逆向替代、置换和线性变换操作。

d. 逆向轮密钥异或：每一轮结束后，将逆向轮密钥与数据块进行异或操作。

e. 输出：输出解密后的数据块。

解密后的数据需要与原始数据进行比对，以确保传输过程中没有发生任何错误。由此采用数字签名实现验证，以确保消息的真实性和完整性。综上所述，完成改进 AES 算法的无线通信网络数据加密安全传输。

3 实验测试

3.1 测试环境的搭建

完成数据加密传输系统的设计和实现后需要对系统的功能进行初步的测试。首先需要搭建网络环境。测试环境下的网络拓扑图如图 5 所示。

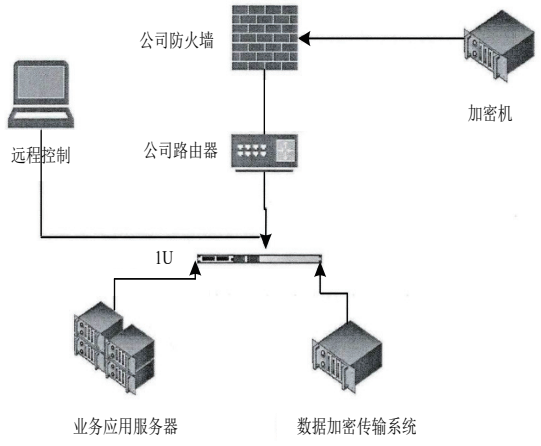


图 5 测试环境网络拓扑图

3.2 测试及结果分析

在上述所搭建的测试环境下，以泄漏概率作为测试指标，选取文献 [2] 方法作为对比方法，展开对所提方法无线通信网络数据传输加密的效果验证。针对泄漏概率指标，分别采用所提方法和对比方法对不同数量的无线通信网络数据进行传输加密，并统计传输后无线通信网络数据的泄漏概率，其结果如表 1 所示。

表 1 泄漏概率对比结果

传输信息量 /bit	所提方法	文献 [2] 方法
1000	2.18%	3.45%
2000	2.32%	3.89%
3000	2.67%	4.05%
4000	2.92%	4.43%

根据表 1 所得结果可知，随着传输信息量的增加，两种方法的泄漏概率均有所增加，但对比两种方法的泄漏概率结果，可得出所提方法的泄漏概率较低，始终维持在 3% 以下。由此可说明，所提方法具有较好的加密效果，可有效实现无线通信网络数据传输加密。

4 结论

为有效降低无线通信网络数据传输加密的泄漏概率，提出基于信任计算的无线通信网络数据传输加密方法。针对 AES 算法中原密钥扩展进行分析，得出其 AES 算法原密钥扩展的缺点，并基于上述分析结果，从减弱密钥字之间的相关性和保留 AES 算法即时性入手，实现改进 AES 算法。最终引入信任计算结果进行无线通信网络数据传输的加密和解码两个过程，完成对无线通信网络数据传输的加密。结果表示，采用所提方法进行无线通信网络数据传输加密方法，其泄漏概率较低，始终维持在 3% 以下，由此说明所提方法具有一定有效性。

参考文献：

[1] 李子健，章国安，陈葳葳 . 基于区块链的车联网安全通信策略 [J]. 计算机工程，2021, 47(10):43-51.

[2] 牛耕 . 基于对称加密的通信网络数据多信道安全传输方法 [J]. 自动化与仪器仪表 ,2022(12):69-72+79.

[3] 张馨方，周江华 . 基于轻量型 AES 加密算法的浮空器平台数据传输方案 [J]. 计算机测量与控制，2023, 31(6):183-190.

[4] 陈家璘，孙志峰，曾铮，等 . 基于透明加密的无线通信网络数据防窃取方法 [J]. 自动化与仪器仪表 ,2022(8):86-90.

【作者简介】

张江鹏（1991—），男，甘肃平凉人，本科，中级工程师，研究方向：信息安全。

（收稿日期：2023-12-05）