基于混沌加密的网络信息安全系统研究

刘 杨 [1]
LIU Yang

摘 要 当前计算机网络通信传输的数据，一般使用传统 RSA、ABE、ECC 等公钥密码系统进行加密，往往存在着算法密钥长度过长、系统性能消耗更高等问题，且局域网通信中一旦系统私钥泄露则公钥立即会被破解。对此，提出基于 Logistic 混沌映射、AES（advanced encryption standard）算法的整形化信息加密系统，通过 Logistics 映射法生成原始明文数据的离散值、使用混沌序列的自适应门限将明文量化为 8 进制序列值。运用 AES 密钥扩展算法进行明文块的密钥加密，可提升网络信息传输与存储管理的安全性。

关键词 混沌加密；网络信息；安全；管理体系

doi：10.3969/j.issn.1672-9528.2024.07.029

0 引言

混沌映射的网络明文数据加密模式，是对传输原始明文数据作出置乱处理、分段线性扰动处理的方式，使网络通信数据形成不规则、离散性的扰动，抵抗外部用户权限访问的选择明文攻击威胁。面向局域网内传输的文本、图像及视频数据信息，设计基于“Logistic 混沌映射 +AES 算法”的数据加密方案，统一定义明文数据的混沌映射序列，使用 AES 算法对包含特定字节长度的明文数据块，作出字节替换、行移位、列混淆、轮密钥加的多轮异或加密操作，经由有线或无线通信网络将加密后的密文传输到后台服务器，以最大程度保障网络信息加密传输的效率与系统安全。

1 大数据环境下网络信息防护管理的安全问题

当前计算机网络通信通常会受到软件木马病毒攻击、DDoS（distributed denial of service）拒绝服务攻击、SQL（structured query language）注入攻击、XML 注入攻击、XSS 跨站脚本攻击等多种类型的攻击问题。传统基于复合型防火墙、Web 应用防火墙的局域网内信息安全防护方案，是利用包含用户源 IP 地址、目的 IP 地址、TCP/IP 协议类型、端口号等信息的深度包过滤规则，验证输入数据包 IP 地址的合法性、限制过滤具有特定端口号或协议类型的数据包进入网络；同时使用路由器或交换机接口中设置的 ACL 访问控制列表，将访问控制列表的SQL查询语句、X.X.X.0/24路由协议、IEEE 802.1 协议应用到网络数据包的访问控制中，作出用户数据包源 / 目的 IP 地址、源 / 目的 Mac 地址、端口通信协议的匹配分析，过滤掉不符合网络地址及访问协议要求的数据包。但 R2U(Remote to User) 远程非授权进入、U2R（user-to-root）非授权访问攻击、DDoS 拒绝服务攻击、Probe 探测攻击等类型的攻击，很大程度上能够绕过 Web 应用网关防火墙的“一次认证与信任服务”授权验证，在一定时间内被赋予更高的信任级别和访问权限，由此带来恶意流量的入侵问题。为避免传统复合型防火墙访问控制认证、数据加密方案，产生的链路节点拦截、传输数据包破解等安全问题，针对网络文本、图像及视频的数据信息，使用“Logistic 混沌映射 +AES 算法”生成随机密钥流进行数据分段线性处理、轮密钥对称加密运算，提升网络传输数据加密的质量、降低网络数据被窃取或丢失的概率 [1]。

2 基于 Logistic 混沌映射的数据置乱、初值扰动处理

网络通信中利用“Logistic 混沌映射 +AES 算法”的数据加密原理为，由内网客户机输入明文数据信息，基于 Logistic 混沌映射模型在明文数据上叠加混沌映射信号，而后使用混沌序列的自适应门限将明文量化为 8 进制序列值，利用混沌映射的伪随机产生器将生成的混沌映射序列作为密钥，利用 AES 算法展开明文数据的加密、解密操作，加密后的密文可在网络通信信道中实现安全传输 [2]。

2.1 基于混沌映射的数据置乱、初值扰动处理

为满足网络计算机信息安全的数据加密需求，选择 Logistic 混沌映射模型对待加密的明文数据信息作出位置置乱处理。假设网络传输的初始明文数据信息为 x_i，混沌迭代函数为 $f(x_i)$，混沌迭代映射的终止值为 K，则按照以下计算公式，完成网络明文数据信息的 Logistic 混沌映射、置乱处理。

1. 河南交通技师学院 河南驻马店 463000

$$x_{i+1}=f(x_i)=\mu x_i(1-x_i)$$
$$\mu=\frac{\sum_{i=1}^{n}(P_s/x_{i+1})}{N\cdot K} \quad (1)$$

$$X=\mu K\cdot\sin^2(x_{i+1}-x_i) \quad (2)$$

式中：μ 为混沌迭代分支参数（控制参数）值，用于表示随着迭代次数增加得到映射数值的离散程度，且通常情况下 $0\leqslant\mu\leqslant 4$。x_i 表示混沌迭代前的明文数据值，x_{i+1} 表示某一次混沌迭代后得到的数值，X 表示混沌迭代的数据置乱处理结果，通常前一混沌迭代计算得到数值作为后一迭代的初始数值。n 表示网络中待加密传输的数据规模，P_s 表示 [0,1] 之间的随机数值；K 分别表示 Logistic 混沌映射最后一次迭代后的值，N 表示混沌映射迭代次数。为避免混沌映射迭代后的终止值 K 与数据初值之间的较大误差，需对置乱结果 X 作出校正处理，计算公式为：

$$\delta=\frac{\left|f(x_{n+1}-x_n)-x_n\right|}{X} \quad (3)$$

式中：δ 表示混沌映射迭代后对终止值 K 的置乱校正。随着控制参数值 μ 的不断增大，混沌映射结果会逐渐呈现出周期性分散状态，但若该周期性分散的混沌状态过短，也即 Logistic 混沌映射存在着短周期现象，那么生成的明文数据信息密钥则很大程度上为弱密钥，进而导致网络信息加密的安全问题 [3]。

为解决这一问题，提出 Logistic 混沌映射的初值扰动处理方案，基本思路为使用 Baker 混沌映射去扰动 Logistic 混沌映射的初始值 x_i。Baker 映射作为一种二维映射方案，可将一维的混沌迭代结果映射到二维平面上的点。按照初始明文数据 x_i、Logistic 混沌映射后的数值 $x_{i+1}=f(x_i)=y_i$，作出 Baker 映射的扰动计算，计算公式为：

$$B(x_j,y_j)=\begin{cases}\left(2x_i,\dfrac{y_i}{2}\right) & 0\leq x_i\leq\dfrac{1}{2}\\ \left(2x_i-1,\dfrac{y_i}{2}+\dfrac{1}{2}\right) & \dfrac{1}{2}<x_i\end{cases} \quad (4)$$

在计算输出经 Baker 映射扰动后的 x_j、y_j 后，按照计算公式（5）计算得到二维映射后的处理结果 O。将 O 作为 Logistic 混沌映射中网络明文数据信息的初始值，依照以上的计算公式（1）、（2）进行混沌映射迭代，可最大程度避免混沌映射陷入短周期现象的问题。

$$O=ax_j+by_j+c \quad (5)$$

2.2 基于混沌映射的序列进制处理、轮密钥流生成

在使用美国联邦政府提出的 AES 数据区块加密标准时，通常要求明文数据的单个分组长度 128 bit 位，加密密钥长度为 128 bit 或 256 bit 位。因而应先将明文数据信息 x 进行分组，每组字节长度为 128 bit 位，再将 128 bit 位的明文数据信息按照 $B_i=\Theta(x_i)=\{0,1\}$ 的计算公式，将分组后的数据转化为 8 或 16 进制序列 $\{B_1,B_2,B_i,\mathrm{K},B_l\}$，单个序列也有固定的序列长度，一般设为 8 bit 或 16 bit 位 [7]。

在 Logistic 混沌映射的校正后混沌序列基础上，使用 $X=\mu K\cdot\sin^2(x_{i+1}-x_i)$ 作为伪随机产生器随机抽取生成的加密密钥流，其中当控制参数 μ=4 时，表明映射序列值完全处于混沌状态，且 Logistic 混沌映射关系均在实数域中实现，因而表明生成的明文数据信息密钥 X 本身的复杂程度更高、在网络通信数据加密中的安全性更强，可被用于 AES 算法的加密操作实践 [8]。

3 基于 AES 对称算法的网络数据信息安全加密执行方案

AES 算法的网络数据信息加密与运算通常经历字节替换、行移位、列混淆、轮密钥加密等多个执行流程，首先基于 Logistic 混沌映射模型、Baker 二维映射法对原始明文数据作出置乱处理，再使用 AES 算法作出明文数据的轮密钥对称加密运算。依照 AES 数据区块加密标准的规定，选择 AES-256 进阶加密标准类型，将本文数据加密的密钥长度设为 8 bit 位，则对应的数据加密迭代次数在 25 次左右 [9]。

3.1 明文数据的字节替换

在完成明文数据固定序列长度的分组后，将单个组内的 $\{B_1,B_2,B_i,\mathrm{K},B_l\}$ 数组，按照 AES 算法中 S（substitution-box）盒的字节置换基本结构（S 盒表），将一定长度（如 16 bit 位）的输入字节映射到较短 (如 8 bit 位）的输出字节中，实际上是对 S 盒表的查表操作过程，其中单个数组序列的前 4 位和后 4 位分别代表行值、列值，具体如表 1 所示 [10]。假设 B1 字节为 0x14，那么该字段前四位的 16 进制为 1，后四位的 16 进制为 4，查找 S 盒表的第 1 行和第 4 列的值，可将字节 0x14 替换为 0xfa。

表 1 明文数据字节替换的 S 盒表查表

0	63	7c	77	7b	F2	6b
1	ca	82	C9	26	fa	59
2	B7	fd	93	26	36	3f
3	04	C7	23	C3	18	96
4	09	83	2c	1a	1b	6e
5	53	D1	00	Ed	20	fc

3.2 数据状态矩阵的行移位

行移位是将明文数据的状态矩阵每行都向左循环移位，通常按照第 i 行左移 i 个字节（i=0,1,2,…）的规则，将第一行左移 1 位、第二行左移 2 位、第三行左移 3 位，移位获得一个新的数据分块。依此类推，经过多次循环移位的变换后得到离散化的分组输入数据，具体执行流程为：

$$\begin{bmatrix} B_{00} & B_{01} & B_{02} & \mathrm{L} & B_{0l} \\ B_{10} & B_{11} & B_{12} & \mathrm{L} & B_{1l} \\ B_{20} & B_{21} & B_{22} & \mathrm{L} & B_{2l} \\ \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} \\ B_{l0} & B_{l1} & B_{l2} & \mathrm{L} & B_{ll} \end{bmatrix} \rightarrow \begin{bmatrix} B_{01} & B_{02} & B_{03} & \mathrm{L} & B_{0(l+1)} \\ B_{11} & B_{12} & B_{13} & \mathrm{L} & B_{1(l+1)} \\ B_{21} & B_{22} & B_{23} & \mathrm{L} & B_{2(l+1)} \\ \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} \\ B_{l1} & B_{l2} & B_{l3} & \mathrm{L} & B_{l(l+1)} \end{bmatrix} \tag{6}$$

3.3 数据状态矩阵的列混淆

列混淆与行移位的计算模式相似，是引入某一固定矩阵，将固定矩阵的行元素与数据状态矩阵移位后的列元素相乘，如将第一行乘以第一列得到首列的第一个元素，第二行乘以第一列得到首列的第二个元素，第 l 行乘以第一列得到首列的第 l 个元素，依此类推，经过多次循环移位的变换后，得到离散化的分组输入数据 [11]。

3.4 轮密钥加密运算

在使用伪随机产生器随机抽取生成的加密密钥流 X 后，所有轮密钥都基于 Logistic 混沌映射模型，从 Round 1 密钥进行扩展生成，选取 Logistic 混沌映射置乱处理后复合序列的前 128 bit 位字节 [12]。而一旦生成密文 $C=[X_f, X_g]$，则管理人员可按照 $m=X_{fi}+X_{gi}$ 的计算公式，从 X_f、X_g 的密钥块中选择第 i 个字节值作为数据状态矩阵 Bi 的加密密钥，其中 C 表示包含 f、g 两个部分的生成密文，X_f、X_g 分别表示加密密钥流的第 f/g 部分，且两个密钥块的长度均为 64 bit 位，m 表示从生成密文的密钥块中选择第 i 个字节值，使之组成数据加密的密钥长度为规定的 8 bit 位 [13]。

对局域网信道内传输的文本、图像及视频等明文数据信息作出多轮的密钥加密运算操作。网络明文数据状态矩阵与轮密钥的异或加密运算，是以列为单位与每一轮密钥进行异或运算，按照这一规则完成数据状态矩阵 $\boldsymbol{B}$、密钥流 X 的异或加密运算，计算公式为式（7），具体执行流程为式（8）。

$$Z_i = \frac{B_i}{\sum E_i \oplus X_i} \tag{7}$$

$$Z = \begin{bmatrix} E_{01} & E_{02} & E_{03} & \mathrm{L} & E_{0(l+1)} \\ E_{11} & E_{12} & E_{13} & \mathrm{L} & E_{1(l+1)} \\ E_{21} & E_{22} & E_{23} & \mathrm{L} & E_{2(l+1)} \\ \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} \\ E_{l1} & E_{l2} & E_{l3} & \mathrm{L} & E_{l(l+1)} \end{bmatrix} + \begin{bmatrix} X_{01} & X_{02} & X_{03} & \mathrm{L} & X_{0(l+1)} \\ X_{11} & X_{12} & X_{13} & \mathrm{L} & X_{1(l+1)} \\ X_{21} & X_{22} & X_{23} & \mathrm{L} & X_{2(l+1)} \\ \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{M} \\ X_{l1} & X_{l2} & X_{l3} & \mathrm{L} & X_{l(l+1)} \end{bmatrix} \tag{8}$$

式中：E 表示网络明文数据状态矩阵的行移位、列混淆运算结果，由此可见，网络明文数据状态矩阵的每个字节元素都要与加密密钥流 X 之间进行对称加密的异或运算。在基于“Logistic 混沌映射 +AES 算法”的网络数据信息加密过程中，即使状态矩阵数据的不同组明文字节值相同，也会因为加密密钥的不同得到不同密文，因而密文不仅与数据明文相关，也与 Logistic 混沌映射的序列值相关，由此能够最大程度避免外部用户访问选择明文攻击 [14]。

4 基于 CHAP 认证协议的混沌映射加密通信认证

在网络链路的混沌映射加密数据通信过程中，引入 CHAP(Challenge Handshake Authentication Protocol) 通信认证协议，是在用户端、后台服务器接收端之间作出三次的身份校验认证，具体的网络通信信息安全识别验证流程如下：

（1）在网络用户进入局域网访问后，由后台认证人员向用户发送端发出“challenge”随机挑战消息。

（2）访问用户接收到后台发送的“challenge”消息后，以 Hash 哈希算法作出访问用户的私钥数字签名、生成端点响应信息，将用户数据包报文 ID、数据加密结果、随机挑战值消息的应答返回至后台。

（3）后台验证方根据收到的应答响应信息，查找系统内的用户 ID 口令、检测随机挑战值消息应答的合法性，若合法则向用户返回成功通信认证信息、否则返回通信认证失败信息。

（4）基于访问用户 ID、数字签名信息，对随机挑战的应答值进行三次握手认证，可最大程度保证网络用户信息访问的安全性。

5 仿真实验及结果分析

5.1 实验环境设置

为验证利用混沌映射算法作出网络加密、通信协议认证的系统信息安全性，基于 Genuine Intel(R) CPU T2080 @1.73 GHz CPU 32 GB 网络计算机，安装 MATLAB R2022a 仿真软件、BitXMesh 测试组件，搭建起实验的软硬件环境。选择 KDD CUP99 公开数据集，从 50 万条数据中随机挑选出 10 条数据作为实验数据集，按照不同明文序列的抗攻击能力设置加密密钥长度，使用混沌映射的伪随机数生成器产生加密

密钥，分析在 R2L 远程非授权访问、DoS 拒绝服务攻击、远程探测性攻击等网络攻击环境下，使用“Logistic+AES”混沌映射加密的网络安全防护质量。

5.2 实验结果分析

基于 MATLAB R2022a 仿真软件，模拟网络信道 CVLAN 端口单位时间内传输的数据流量，使用“Logistic 混沌映射 +AES 算法”作出信道节点的明文数据加密，设置单个加密密钥长度为 8 bit 位，控制参数 μ=4，数据加密迭代次数为 25 次左右，实时监控单位时间内网络端口的非法访问、攻击数据包等业务流量变化情况，并与 KP-ABE 属性基算法的密钥加密策略作出比较分析，实验结果如表 2、图 1 所示。

表 2 基于“Logistic 混沌映射 +AES 算法”的网络信息安全加密结果

数据吞吐量（TPS）	＜ 100 kB	＜ 1000 kB	＞ 10 MB
加密速度	＜ 0.01 s	＜ 0.1 s	＜ 1 s
PBET 容错	70%	80%	90% 以上

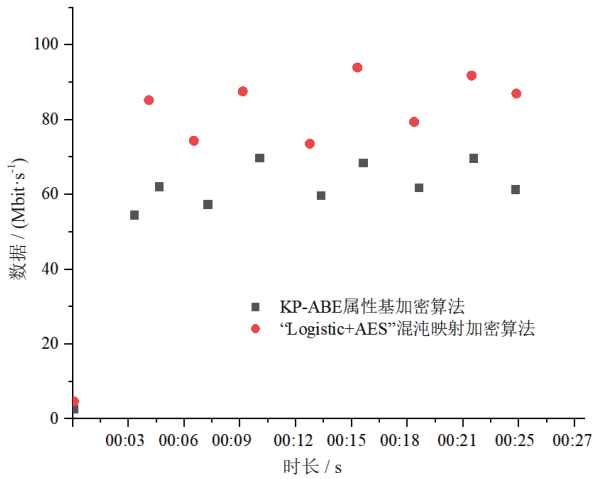

图 1 “Logistic 混沌映射 +AES 算法”与 KP-ABE 算法的单位时间内加解密数据量

根据表 1 可得出，在小于 1000 kB 的数据吞吐量（TPS）范围内，使用“Logistic 混沌映射 +AES 算法”的网络数据信息加密方案，无论是加密验证速度还是 PBET 容错，都呈现稳步上升的趋势，其中在大于 10 MB 的数据吞吐量（TPS）情况下算法加密验证速度在 1 s 左右，PBET 容错上升至 90% 以上，表明前期加密数据速率快，但容错率低，且算法加密及验证的疏漏问题严重，但加密数据量大于 1 MB 的情况明显改善。从图 1 可以发现，在 25 s 时间内利用“Logistic 混沌映射 +AES 算法”的混沌加密方案，单位时间内加解密数据量要远远高于 KP-ABE 算法，且加密验证的成功率也更高，表现出“Logistic 混沌映射 +AES”算法加密的明显优势。

6 结语

传统基于 DES、RSA、ABE、ECC 等的对称或非对称加密算法方案，通常面向网络通信链路或节点加密设置系统公钥、加解密私钥，作出网络节点或传输数据本身的加解密操作，但若入侵攻击用户一旦拦截和破解加密密钥，则会对网络信道内的传输数据作出拦截、窃取和篡改破坏。因此，基于 Logistic 混沌映射、AES 算法建构网络信息加密体系，利用内网信源节点采集客户机输入的明文数据信息，按照 AES 算法设定的迭代次数对数据块作出混沌序列轮密钥的加密和解密运算，能够消除数据传输并行加密过程中过渡态的影响，抵抗网络通信过程中选择明文攻击问题。

参考文献：

[1] 冯伟，张靖，秦振涛，等 . 基于变步长约瑟夫遍历和 DNA 动态编码的图像加密算法的安全性分析 [J]. 电子与信息学报，2022, 44(10):3635-3642.

[2] 曹梦川，伍丹，杜朋轩 . 基于非对称加密算法的农业物联网数据加密解密模块的研究 [J]. 信息与电脑 (理论版), 2022(15): 224-228.

[3] 朱淑芹，李秀娟，李若玉 . 对一种基于动态 S 盒与混沌映射的图像加密算法的安全分析与改进 [J]. 中国电子科学研究院学报 ,2022(2):162-169.

[4] 李小明 . 基于混沌映射进行数据加密的安全电子邮件系统研究 [J]. 现代电子技术 ,2021,44(11):37-41.

[5] 田军锋，彭静静，左宪禹，等 . 基于循环移位和多混沌映射的图像加密算法 [J]. 计算机科学 ,2020,47(10):327-331.

[6] 蒋东华，朱礼亚，沈子懿，等 . 结合二维压缩感知和混沌映射的双图像视觉安全加密算法 [J]. 西安交通大学学报，2022, 56(2):139-148.

[7] 王娇婷 . 辽宁广电行业网络安全态势感知平台研究与设计 [J]. 电子世界 ,2021(24):67-68.

【作者简介】

刘杨（1983—），女，河南驻马店人，本科，二级实习指导教师，研究方向：计算机应用和网络安全。

（收稿日期：2024-04-25）