基于 RSA 的通信工程环境安全监测设计研究

刘宇萌 [1]
LIU Yumeng

摘 要 基于 RSA 算法，针对通信工程环境中的安全监测问题进行了设计和研究。通过对 RSA 算法的原理和特点进行分析，提出了一种基于 RSA 的通信工程环境安全监测方案。利用 RSA 算法的非对称加密和数字签名功能，实现了对通信数据的加密和认证，从而确保通信过程的安全性。通过实验验证，所提出的方案在保障通信工程环境安全方面具有较好的效果。

关键词 RSA 算法；通信工程；安全监测

doi：10.3969/j.issn.1672-9528.2024.08.025

0 引言

随着信息技术的快速发展，通信工程环境中的安全问题日益突出。网络攻击、数据泄露等安全威胁给通信工程环境的稳定运行和数据传输带来了严重的挑战 [1]。为了解决这一问题，本研究从加密和认证两个方面出发，基于 RSA 算法设计了一种通信工程环境安全监测方案。通过对 RSA 算法的原理和特点进行深入研究，本研究旨在提供一种有效的安全监测解决方案，以保障通信工程环境的安全性。

1 通信工程环境网络数据加密

通信工程环境网络数据加密是一种保护通信数据安全的重要技术。加密通信工程环境网络数据的具体步骤如表 1。

表 1 加密通信工程环境网络数据的具体步骤

步骤	内容
步骤 1	随机选取两个大素数 x 和 y，并且确保 $x \neq y$。然后，通过求解 $n=x \times y$，得到一个大的合数 n。这一步骤是为了构建 RSA 算法所需的公钥和私钥。
步骤 2	利用欧拉定理获取 n 的欧拉函数值，记为 $\varphi(m)$。欧拉函数是指小于 m 且与 m 互质的正整数的个数。根据欧拉定理，当 m 为素数时，$\varphi(m)=m-1$。因此，通过计算 $\varphi(m)$，得到 n 的欧拉函数值。
步骤 3	计算 $\varphi(n)$ 的乘法逆元 d，即满足 $d \cdot e \equiv 1 (\mathrm{mod}\ n)$。其中，mod 代表求余运算符。通过计算得到的 d，用于构建 RSA 算法的私钥。
步骤 4	公钥 (e, n) 中的 e 是在步骤 3 中选取的整数，而 n 是在步骤 1 中计算得到的大合数。私钥 (d, n) 中的 d 是在步骤 3 中计算得到的乘法逆元，而 n 与公钥中的 n 相同。
步骤 5	使用公钥 (e, n) 来加密数据。将待加密的数据 m 与公钥中的 e 进行运算，得到加密后的数据 c，数据 m 就被成功加密成 c。

1. 西安交通工程学院 陕西西安 710000

其中，RSA 加密算法被广泛应用于数据加密过程中。然而，RSA 算法的安全性与大素数的选择密切相关 [2]。为了改进 RSA 算法的安全性，利用概率性算法中的 Solovay-Strassen 算法来判定 RSA 加密过程中的大素数。

为了确保选取的素数满足素数的条件，利用概率性算法中的 Solovay-Strassen 算法进行判定。Solovay-Strassen 算法是一种用于判定一个给定的数是否为素数的概率性算法。通过对选取的大素数进行 Solovay-Strassen 算法的验证，确定它们是否满足素数的条件。Solovay-Strassen 算法基于费马小定理和欧拉准则，通过进行一系列的随机测试来判断一个数是否为素数。这些随机测试能够在很高的概率下确定一个数是否为合数，但并不能完全排除存在的伪素数。

2 通信工程环境网络异常行为判断

信息熵是用来度量数据的不确定性和随机性的指标。在网络流量分析中，将网络流量数据转换为信息熵的形式，以更好地描述数据的复杂性和变化性。通过对源 IP 地址、目的 IP 地址、源端口号和目的端口号进行统计和计算，得到每个时间点的熵值，就得到了四个熵时间序列，分别表示源 IP 地址、目的 IP 地址、源端口号和目的端口号的变化情况。接下来，利用这四个熵时间序列，建立网络流量异常行为判断的时间序列图。时间序列图是一种用于展示数据随时间变化的图表。在网络流量异常行为判断中，将时间作为横轴，熵值作为纵轴，绘制四个熵时间序列的曲线。通过观察时间序列图，发现异常行为对应的熵值变化情况。例如，当某个熵时间序列的熵值突然增大或减小，或者出现明显的波动和异常值时，就表示网络流量存在异常行为。建立时间序列图主要包含两部分，分别是点与边的表示。

首先，将加密后的通信工程环境网络流量信息熵的取值进行归一化处理，将其映射至范围 [0, 1] 内。通过线性变换或者其他归一化方法，将原始的熵值转换为 0 ～ 1 之间的标准化值。接下来，根据映射后的取值，将信息熵划分为不同的等级。根据题目中给出的等级划分，将范围 [0, 0.35）划分为等级Ⅰ，范围 [0.35, 0.7）划分为等级Ⅱ，范围 [0.7, 1] 划分为等级Ⅲ。等级Ⅰ表示信息熵较低，即网络流量的变化和复杂性相对较小，代表着较为正常的流量行为。等级Ⅱ表示信息熵适中，网络流量的变化和复杂性处于中等水平，存在一些轻微的异常行为。等级Ⅲ表示信息熵较高，网络流量的变化和复杂性较大，存在较为严重的异常行为。

假设 a 和 β 是一个 2- 项集，且 a、B=A、B、C、D，$\alpha \neq \beta$。同时，am 是一个 3- 项集，其中 Ha、β、n = A、B、C、D，$a \neq B$，$B \neq n$，$\alpha \neq n$。这些点之间的模式 m 是一个 3- 项集模式，其信息熵的取值所处的等级表示为 i、1 和 k。通信工程环境中的网络流量异常行为通过时间序列图像中较为奇怪的项集模式来判断。在时间序列图中，如果出现了与正常模式不符的、较为奇怪的项集模式，就表示存在网络流量的异常行为。通过对网络流量的源 IP 地址、目的 IP 地址、源端口号和目的端口号进行分析，得到信息熵模式，并将其映射至不同的等级。同时，通过对 2- 项集和 3- 项集的分析，进一步确定网络流量的异常行为。根据异常行为的贡献程度和时间点的特征，采取针对性的措施，如增加网络监控、加强安全防护、优化系统配置等，以应对网络流量的异常行为。网络流量异常行为异常程度 U_t 的公式为：

$$U_t = \min_{0<t<N} \log_{10}\Big(\sum_{1\le\alpha,\beta\le3,\alpha\neq\beta}\omega^2_{\alpha,\beta}\times\lambda Sup_t(\alpha,\beta)+0.5\times \sum_{1\le\alpha,\beta,\eta\le3,\alpha\neq\beta,\alpha\neq\eta,\beta\neq\eta}\omega^3_{\alpha,\beta,\eta}\times\lambda Sup_t(\alpha,\beta)\Big) \tag{1}$$

式中：t 是网络流量时间序列图所处时间点，N 是总时间点数。

3 通信工程环境网络攻击检测

针对通信工程环境异常网络流量 Z'_i 和 $Z'_{j'}$ 求解时间点时，Z'_i 和 $Z'_{j'}$ 的相关系数 $cof(i', j', t)$：

$$cof(i', j', t) = \max corrocofe(Z'_i(t), Z'_{j'}(t_{j'}))r_2 \tag{2}$$

式中：Z'_i 以 t 为中心，r_2 为半径的时间区域 Z'_i 和 $Z'_{j'}$ 的相关系数是：

$$\max corrocofe(Z'_i(t), Z'_i(t_{j'})) \tag{3}$$

则成立条件为：

$$\begin{cases} 0 \le t \le T - r_1 + 1 \\ t - r_2 \le t_{j'} \le t + r_2 \\ i' \neq j' \end{cases} \tag{4}$$

获取平均相关系数序列 $meancof(t)$，其公式为：

$$meancof(t) = \frac{\sum_{i'}\sum_{j'}\sum_{t} cof(i', j', t)}{\varsigma} \tag{5}$$

式中：ς 是异常网络流量链路总数，$0 \le t \le T - r_1 + 1$，$i' \neq j'$。

网络攻击检测流程如图 1 所示，cof 作为一种衡量网络流量之间相关性的指标，用来判断网络流量是否正常。通过对异常网络流量历史时间段的 cof 分布情况进行分析，得到不同网络攻击类型的 cof 分布特征。利用 $meancof(t)$ 对相关系数设定门限的过程如下。

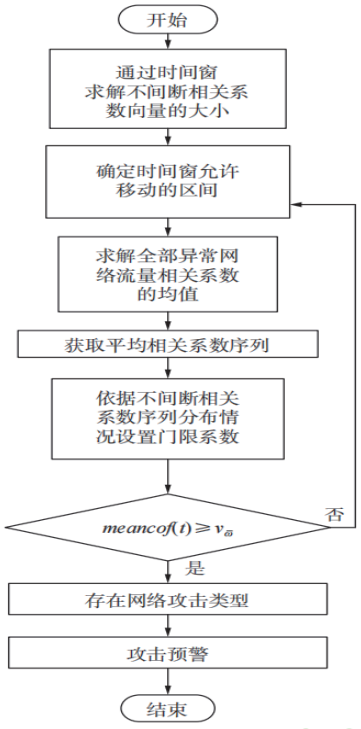

图 1 网络攻击检测流程

首先，收集一段时间内的通信工程环境网络流量数据，并计算出每个时间点的 cof 值。然后，对这些 cof 值进行统计和分析，得到它们的均值 $meancof(t)$。接下来，根据不同网络攻击类型的 cof 分布特征，设定相应的门限系数。门限系数的设定需要根据具体情况进行调整。一般而言，如果网络流量的 cof 值超过门限系数，就判断为异常或受到网络攻击。不同类型的网络攻击对应不同的门限系数。例如，对于 DoS 攻击，需要设置较低的门限系数，因为 DoS 攻击会导致网络流量的相关性降低。而对于 DDoS 攻击，需要设置较高的门限系数，因为 DDoS 攻击会导致网络流量的相关性增加。令该历史时间段内 cof 的均值是 $\overline{cof}$，方差是 δ^2，门限系数是 ξ_{ϖ}，门限是 V，则：

$$V = meancof(t) + \xi_{\varpi} \cdot \delta^2 \tag{6}$$

式中：通信工程环境网络攻击类型是 ϖ，利用 V 衡量 $meancof(t)$。

4 实验分析

首先，随机选择一段网络数据作为实验样本。这段网络数据包含了一定时间范围内的通信工程环境网络流量信息。将这段网络数据划分为多个时间点，每个时间点代表了 10 分钟内的网络数据。接下来，将使用本文方法、文献 [3] 方法和文献 [4] 方法对这段网络数据进行加密处理。每种方法都有不同的加密算法和策略，保护网络数据的安全性和隐私性。然后，将测试本文方法加密后的字符频率变化情况。通过对加密后的网络数据进行字符频率分析，了解加密后的数据中各个字符出现的频率变化情况。如果加密后的字符频率与原始数据相比发生了显著的变化，说明本文方法对网络数据进行了有效的加密处理。最后，将根据字符频率的变化情况来衡量本文方法的网络数据加密效果。如果加密后的字符频率变化明显，且与原始数据的频率分布不可逆推，那么认为本文方法对网络数据进行了有效的加密，提高了数据的安全性和保密性，分析结果如图 2 所示。

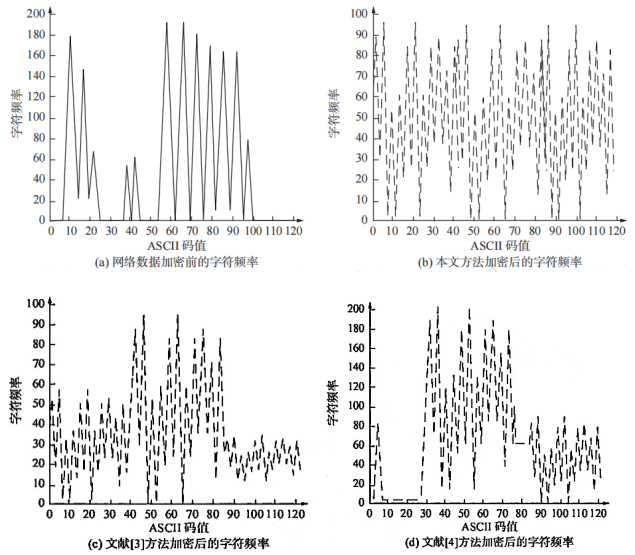

图 2 网络数据加密效果

通信工程环境网络数据加密前的明文字符 ASCII 码值在 8 ～ 25、37 ～ 45、53 ～ 100 左右的字符频率波动较大，这说明在这些 ASCII 码值区间内存在较为重要的网络数据。这些字符频率的波动意味着这些特定的 ASCII 码值对于网络数据的传输和处理具有重要的意义，包含了敏感信息或关键数据。另外两种方法在加密过程中产生了不可预测的字符变化，导致密文字符的频率分布不均匀。这种不均匀的分布情况会给攻击者提供一些线索或机会来破解加密算法，从而危及网络数据的安全性。本文方法能够有效地隐藏明文字符的频率波动，并使密文字符的分布更加均匀。本文方法能够提升网络数据存储的安全性，保护敏感信息和关键数据免受未经授权的访问。

攻击前后网络流量信息熵序列如图 3 所示，在时间点为 60 ～ 80 和 120 ～ 140 时，异常系数时序图显示出两个尖峰，这说明在这两个时间段内，通信工程环境网络流量存在异常行为。这些异常行为是由网络攻击或其他不正常的网络活动引起的。这与实际注入网络攻击的时间点一致，进一步验证了网络流量异常的存在。

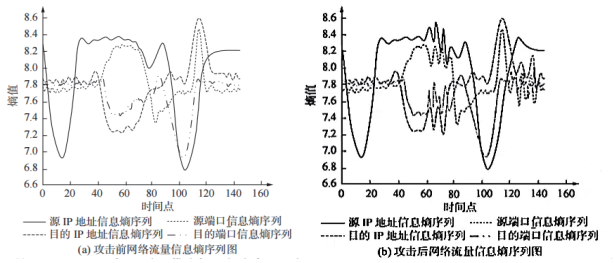

图 3 攻击前后网络流量信息熵序列图

然而，文献 [3] 方法和文献 [4] 方法在异常行为的诊断方面存在一些问题。首先，它们的异常行为时间范围过大，无法精确定位到具体的异常时间段。其次，它们的异常行为诊断准确性较低，会将一些正常的网络活动误判为异常行为，或者忽略一些真正的异常行为 [5]。相比之下，本文方法在判断网络流量异常行为方面更加精准。通过分析异常系数时序图，本文方法能够准确地定位到网络流量异常行为发生的时间段，并且能够排除一些正常的网络活动对异常判断的干扰。这使得本文方法在网络流量异常行为的识别和分析方面具有更高的准确性和可靠性。网络流量异常系数、攻击检测结果如图 4 和图 5 所示。

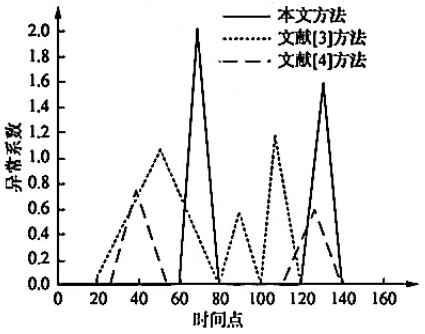

图 4 网络流量异常系数时序判断结果

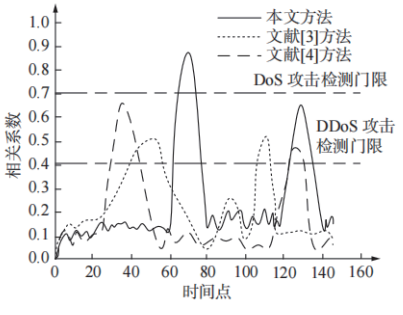

图 5 网络攻击检测结果

本文方法在通信工程环境网络流量的异常行为判断方面表现出了精准性。本文方法能够准确地判断出网络流量的异常行为，并能够区分不同类型的网络攻击。这使得本文方法能够精确地检测到 DoS 攻击和 DDoS 攻击等常见的网络攻击类型。首先，本文方法通过对网络流量的特征进行深入分析，建立了一套准确的异常行为检测模型。该模型考虑了多个关键特征，以及流量之间的关联性。通过对这些特征进行综合分析，本文方法能够准确地判断出异常行为，并能够区分不同类型的网络攻击。其次，本文方法采用了一系列高效的算法来处理和分析网络流量数据。这些算法包括机器学习算法、数据挖掘算法和统计分析算法等。通过对网络流量数据进行大规模的分析和处理，本文方法能够识别出异常行为并进行准确的分类。这使得本文方法在网络攻击检测方面表现出了较高的精准性。同时，本文方法还考虑了一些正常的网络活动对异常行为和攻击检测的干扰。通过建立正常行为模型，并对网络流量数据进行实时比对，本文方法能够排除一些正常的网络活动对异常行为和攻击检测的干扰。这提高了检测结果的准确性和可信度 [6]。

如图 6 所示，本文方法展现出了快速处理数据的能力。它利用高效的算法和优化的加密策略，能够在较短的时间内完成加密操作。

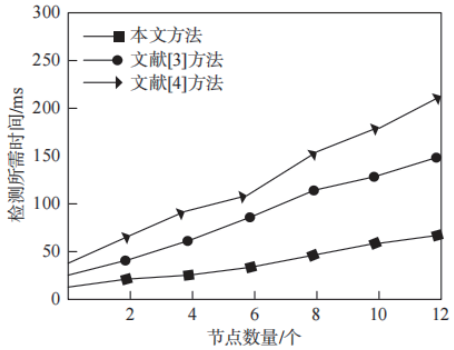

图 6 不同算法攻击检测时间对比

不仅如此，本文方法还能够处理大量的密文属性，而不会因为属性数量的增加而导致加密时间的显著增长 [7]。首先，本文方法采用了高效的加密算法和策略，能够在加密过程中迅速处理数据。通过优化算法的设计和实现，本文方法能够在较短的时间内完成加密操作。这使得在实际应用中，本文方法能够快速、高效地完成加密任务，提高了系统的响应速度 [8]。其次，本文方法具备处理大量密文属性的能力。密文属性是加密过程中的重要组成部分，而且在某些应用场景中，密文属性的数量可能非常庞大。然而，本文方法能够处理大量的密文属性，而不会因为属性数量的增加而导致加密时间的显著增长。这得益于本文方法的优化策略和算法设计，使得在大规模密文属性的情况下，加密时间仍能保持在可接受的范围内 [9]。在检测过程中，本文方法同样具备出色的时间性能。它能够迅速地对加密后的数据进行解密和检测操作 [10]。本文的方法采用代理重加密过程简化形式，使得解密和检测过程不会占用过多的时间。即使在密文属性数量增加的情况下，本文方法所需的时间也不会显著增长。这使得在实时性要求较高的场景中，本文方法具备了很大的优势。

5 结语

本研究基于 RSA 算法，设计了一种针对通信工程环境的安全监测方案。通过对 RSA 算法的应用，实现了对通信数据的加密和认证，从而确保了通信过程的安全性。通过实验验证，该方案在保障通信工程环境安全方面具有较好的效果。然而，本研究还存在一些局限性，如对于大规模通信系统的适用性有待进一步研究。未来的研究需进一步优化和改进该方案，以适应不同规模和复杂度的通信工程环境。总体而言，本研究为通信工程环境的安全监测提供了一种有效的解决方案，对于保障通信系统的安全性具有重要的意义。

参考文献：

[1] 谢凯，代康．基于 RSA 算法的无线异构通信网络数据加密传输方法 [J]. 长江信息通信 ,2023,36(8):118-120.
[2] 杨博麟，张帆，赵运磊，等．针对 AKCN-MLWE 算法的故障攻击 [J]. 计算机学报 ,2023,46(7):1396-1408.
[3] 徐凯，宣涵，陆煜斌，等．弹性光网络中结合预测的多维感知 RSA 算法 [J]. 光通信技术 ,2021,45(4):43-47.
[4] 肖勇，钱斌，蔡梓文，等．电力物联网终端非法无线通信链路检测方法 [J]. 电工技术学报 ,2020,35(11):2319-2327.
[5] 承昊新，王康，夏凌，等．电力物联网终端无线通信链路检测方法分析 [J]. 中国新通信 ,2022(8):10-12.
[6] 苏蓓蓓，黄星杰，尚智婕，等．基于 RSA 算法的计算机网络通信安全加密方法 [J]. 现代传输 ,2022(3):66-68.
[7] 王鑫淼，孙婷婷，马晶军 .RSA 算法在网络数据传输中的研究进展 [J]. 计算机科学 ,2023,50(S1):703-709.
[8] 贾斌斌，王忠庆，方炜．对提高 RSA 算法中大数模乘运算速率的思考 [J]. 信息通信技术与政策 ,2023,49(6):84-90.
[9] 魏秀岭，吕建新，杜传祥，等．基于三素数改进 RSA 算法的智能小区数据信息保护研究 [J]. 冶金管理 ,2020(15):22-23.
[10] 韩宝杰，李子臣．基于 SM2 与 RSA 签密的秘密共享方案 [J]. 通信技术 ,2020,53(8):1976-1982.

【作者简介】

刘宇萌（1995—），女，山西运城人，本科，助理实验师，研究方向：通信工程。

（投稿日期：2024-05-15）