基于 RSA 算法的无线异构通信网络数据加密传输方法

谢　凯，代　康
（新疆工程学院 信息工程学院，新疆 乌鲁木齐 830000）

摘要：为提高数据传输过程中的安全系数，引进 RSA 算法，对无线异构通信网络数据加密传输方法展开设计研究。采用模拟通信信道的方式，通过微分变换算法，实现对无线异构通信网络数据传输的预处理与伪代码生成；引进 RSA 算法，设定无线异构通信网络数据加密传输中的子密钥，实现数据的安全通信与传输。对比实验结果证明：设计的加密传输方法应用效果良好，提高了无线异构通信网络节点的安全系数，为通信过程中的数据安全提供进一步的保障。

关键词：RSA 算法；双向认证；子密钥；传输方法；数据加密；无线异构通信网络
中图分类号：TP309.7　　**文献标识码：**A　　**文章编号：**2096-9759(2023)08-0118-03

Data encryption transmission method of wireless heterogeneous communication network based on RSA algorithm

XIE Kai，DAI Kang
(School of information engineering, Xinjiang Institute of Engineering 830000, China)

Abstract: In order to improve the security factor in the process of data transmission, RSA algorithm is introduced to design and study the data encryption transmission method of wireless heterogeneous communication network. The method of analog communication channel and differential transformation algorithm are used to realize the preprocessing and pseudo-code generation of data transmission in wireless heterogeneous communication network; RSA algorithm is introduced to set the sub-key in the data encryption transmission of wireless heterogeneous communication network to realize the safe communication and transmission of data. The comparative experimental results show that the designed encryption transmission method has good application effect, improves the security coefficient of wireless heterogeneous communication network nodes, and provides further guarantee for data security in the communication process.

Key words: RSA algorithm; Two-way authentication; Subkey; Transmission method; Data encryption; Wireless heterogeneous communication network

0 引言

无线异构通信网络是构成互联网的基础，一个完整的局域互联网可以由多个无线异构通信网络构成，用于连通网络、保障各区段通信的设备为路由器[1-2]。当数据在网络中传输时，如果通信对端未能及时采取有效的措施，对通信过程进行安全保障，不仅会导致传输过程中的数据受到外界环境的影响出现丢失、被窃取等异常，还可能会遭遇到以下几种攻击：不正当的用户冒充合法的用户，对数据通信传输过程进行非法访问；对敏感资料的违法窃取、对窃取的资料进行任意修改，造成接收资料的畸变，甚至彻底损坏等。

为解决此方面问题，提高网络数据传输中的安全性与可靠性，全面保障数据传输安全，有关研究人员在开展了大量研究后，提出了可用于数据加密的多种技术，包括大数据技术、云计算技术等，尽管提出的技术可以实现在网络通信过程中对终端用户身份的验证、非法访问的控制，但根据设计方的反馈可知，现有的大部分加密技术在实际应用中都存在一定的局限性[3]。

为此，本文将在研究中，引进 RSA 算法，以无线异构通信网络为例，对数据加密传输方法展开设计研究，旨在通过此次设计，为异构网络数据传输过程中的隐私数据给予安全保障。

1 无线异构通信网络数据传输预处理与伪代码生成

为实现对数据的加密传输，保障用户在无线异构通信终端上的信息的安全性与隐私性，需要在加密前，对无线异构通信网络数据传输进行预处理[4]。使用微分变换算法，在前端将一个完整的数据包划分成若干个数据包，每个划分后形成的数据包均可作为一个独立的数据包，在无线异构通信网络中进行数据包的映射，可以得到一个待传输的镜像数据文件，在此种条件下，计算数据包的属性，计算公式如下。

$$x_{n+1}=y\cdot x_n(1-x_n) \tag{1}$$

公式(1)中：x_{n+1} 表示待传输的镜像数据文件属性；y 表示 Logistic 映射空间；x_n 表示原始数据包属性。完成数据包的预处理后，需要在数据的发送端生成一个伪数据代码，根据待传输数据包的特点，对伪代码在 Logistic 空间中映射，此过程如下计算公式所示[5]。

$$s=R(32) \tag{2}$$

公式(2)中：s 表示生成的伪代码在 Logistic 空间中映射；R 表示代码生成标准；32 表示代码的位数。按照上述方式，完成无线异构通信网络数据传输预处理与伪代码生成。

2 基于 RSA 算法设定数据加密传输子密钥

引进 RSA 算法，设定无线异构通信网络数据加密传输中的子密钥[6]。在此过程中，需要随机选择两个素数，将其表示为 a 与 b，将 a 与 b 作为数据包加密传输中核心信息的提取标准，在确保 a 不等于 b 的条件下，设定传输数据包中的核心数据提取函数，此过程如下计算公式所示[7]。

收稿日期：2023-03-17
作者简介：谢凯(1978-)，男，汉族，山东巨野人，本科，讲师，研究方向：通信工程。

$$\begin{cases} f = a \cdot X \cdot b \\ \varphi(f) = (a-1) \cdot X \cdot (b-1) \end{cases} \tag{3}$$

公式（3）中：f 表示针对待传输数据包中核心数据的提取函数；X 表示待传输数据包；φ 表示数据迭代行为。将现有的数据划分为两类，分别为核心信息与非核心信息，提取核心信息，将其作为传输过程中的主要加密信息[8]。在 f 的基础上，将 a 与 b 作为两个因数，对其进行自拆解。设定 RSA 算法的最大素数长度为 100 位，可采用十进制机制，对 f 进行数据聚拢，确保数据聚拢到 200 位以下，输出此时的 a 与 b，可以将 a 与 b 作为 RSA 算法加密过程中的最强加密素数，令 a-1 和 b-1 的公因子达到极小值后，$(a+b)/2=1$ 将成立，在此种条件下，可以将 a 与 b 作为 RSA 算法的加密参数。参照上述标准，进行子密钥的设定，此过程如下计算公式所示[9]。

$$G' = \mathrm{mod}(f) \tag{4}$$

公式（4）中：G' 表示数据加密传输子密钥。按照上述方式，完成基于 RSA 算法设定数据加密传输子密钥。

3 密钥更新与数据加密传输中的双向认证

根据数据加密传输的需求，可按照下述公式，生成一个随机数，对加密传输中的子密钥进行更新。

$$S = \sum_{l>1}^{h} h_l \cdot P_l \tag{5}$$

公式（5）中：S 表示密钥更新；h 表示公钥矩阵；l 表示密钥长度；P 表示随机数。计算过程中应明确，所有的公钥、私钥都是与时间戳相关的，且是由通信方自身产生的[10]。在上述内容基础上，提取通信过程中信息发送端用户的物理 MAC 地址与随机数生成信息，向对端发送通信请求[11]。利用 ECDH 算法协商的密钥形成密文，通信方在收到消息之后，利用共享密钥对其进行解密，从而得到发送方的 MAC 地址和随机数[12]，实现对双方身份信息的认证，实现数据的安全通信与传输。

4 对比实验

为满足实验需求，选择某科研单位作为此次研究的试点单位，在测试环境中按照规范部署无线异构通信网络，将网络覆盖区域作为实验区域。按照此种方式，搭建如图 1 所示的对比实验环境。

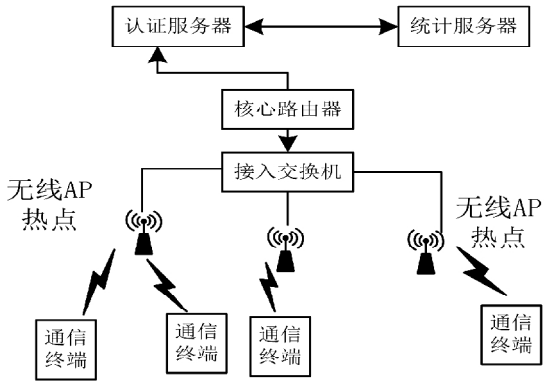

图 1 无线异构通信网络环境

无线异构通信网络由核心路由器连接，为确保搭建的实验环境满足实际工作需求，应对实验环境中的核心路由器进行选型，核心路由器技术参数如表 1 所示。

表 1 核心路由器参数

序号	项目	参数
（1）	CPU	4 核心 2.2GHz ARM 处理器
（2）	FLASH	8GB emc
（3）	SDRAM	2GB DDR3
（4）	光接口	2 个 10G SFP
（5）	电接口	4 个 10/100/1000M 自适应 LAN；1 个 10/100/1000M 自适应 WAN；1 个 Console
（6）	PD 接口	1 个 10/100/1000M 自适应 PD 接口，支持 IEEE8023bt POE+标准
（7）	端口 WAN/LAN 转换	支持
（8）	SIM/UIM 卡接口	2 个 SIM 卡槽，支持 1.8V/3V SIM/UIM 卡，内置 15KV ESD 保护
（9）	WLAN 频段	2412-2484MHz；5150~5825MHz
（10）	无线模式	支持 AP、APWS、Station、Station WDS、中继模式
（11）	Multi-SSID	每个 Radio 最多支持 8 个 ESSID

随机选择一个通信节点，记录通信过程中发送端数据包形式与传输节点数据包的形式，将其作为检验本文方法数据加密效果的关键指标之一，其结果如图 2 所示。

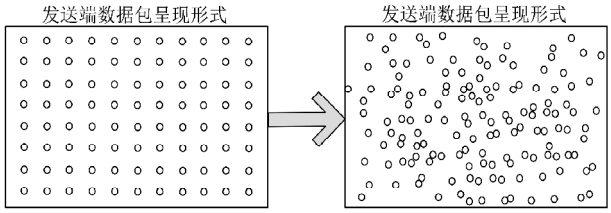

图 2 发送端数据包呈现形式与传输节点数据包呈现形式

从图 2 所示的内容中可以看出，使用本文设计的方法进行数据加密处理后，可以使数据在无线异构通信网络中传输呈现无序状态，避免秩序化数据在网络中传输存在被篡改、被盗用等风险。

在上述内容的基础上，引进基于 IPFS 算法与 Ethereum 的加密传输方法、基于递归神经网络的加密传输方法，将提出的两种方法作为传统方法 1 与传统方法 2，使用传统方法与本文方法，进行无线异构通信网络数据的加密传输。计算使用三种方法进行数据加密后，传输过程中节点数据的安全系数。计算公式如下。

$$\tau = \sum_{J>1}^{J} A \times g_J \tag{6}$$

公式（6）中：τ 表示数据加密传输过程中节点数据的安全系数；A 表示通信网络稳定系数；g 表示网络环境通信条件；J 表示无线异构通信网络中的有效节点，取值通常为>0 的正整数。在上述设计内容的基础上，对计算结果 τ 进行量化，根据 τ 的不同取值，进行三种方法加密效果的分析，相关内容如表 2 所示。

表 2 量化标准与代表含义

序号	取值范围	加密传输过程中的安全性描述
（1）	0~0.2（含 0.2）	安全性极差，几乎无防护
（2）	0.2~0.4（含 0.4）	安全性较差，存在数据被篡改、被窃取等风险
（3）	0.4~0.6（含 0.6）	安全性中等，防护效果无法达到预期
（4）	0.6~0.8（含 0.8）	安全性较好，应用方法可以起到安全防护效果，但无法抵御等级较高危险的攻击
（5）	0.8~1.0（含 1.0）	安全性极好，可以实现对数据安全的全面保障

基于 KNN 算法的计算机网络入侵数据识别方法

张创基[1]，林伟烜[2]，陈运胜[1]
（1.广州华立科技职业学院；2.广州华商职业学院，广东 广州 511325）

摘要：针对传统算法在识别网络入侵数据时，易出现识别正确率、分类正确率偏低的问题，提出基于 KNN 算法的计算机网络入侵数据识别方法。针对被入侵的计算机网络，以预处理后的网络数据为基础，对其中的异常数据实施分类处理；然后，利用 KNN 算法分析数据中的离群点，并找到异常数据间的关联信息和分布规律；最后，构建入侵行为识别模型，在网络遭受同类别的网络入侵行为时，可以实现对入侵数据的实时检测。实验结果表明：与传统的识别方法相比，基于 KNN 算法的识别方法提高了对网络入侵数据的识别准确率。

关键词：KNN 算法；计算机网络；入侵数据；入侵识别
中图分类号：TP391　　**文献标识码：**A　　**文章编号：**2096-9759（2023）08-0120-03

0 引言

随着科技与社会的发展，网络安全的重要性日益凸显。互联网的运营和开发环境正在逐步改变。在保证网络安全的前提下，对网络进行入侵检测是保证网络安全的一个重要环节，其已经成为科技应用的安全工具，是网络安全维护工作中的重中之重[1]。

入侵数据识别是对恶意、可疑的活动进行分类与识别，并做相应的处理。网络入侵数据识别方法包括特征的选择与训练。高效的特征选择能够在大规模数据中过滤掉大量误导性数据，筛选出有效的关键特征。

基于上述分析，本文提出了一种基于 KNN 算法的计算机网络入侵数据识别方法。

1 方法设计

1.1 网络数据预处理

历史入侵数据预处理的过程如图 1 所示。

收稿日期：2023-04-06
作者简介：张创基（1983-），男，广东揭阳人，工程硕士，副教授，研究方向：计算机网络安全、大数据等。

按照上述方式，统计三种方法在实际应用中的加密传输效果，相关内容如表 3 所示。

表 3　加密传输效果

序号	传输方向	本文方法加密传输（τ）	传统方法 1（τ）	传统方法 2（τ）
（1）	1→2（2→1）	0.96	0.65	0.56
（2）	1→3（3→1）	0.95	0.76	0.55
（3）	1→4（4→1）	0.98	0.78	0.53
（4）	2→3（3→2）	0.96	0.79	0.50
（5）	2→4（4→2）	0.92	0.71	0.59
（6）	3→4（4→3）	0.91	0.76	0.58

从表 3 所示的实验结果可以看出，使用本文方法进行数据加密传输，传输过程中节点数据安全系数>0.9，安全性极好。使用传统方法 1 进行数据加密传输，传输过程中节点数据安全系数在 0.6~0.8 之间，安全性较好。使用传统方法 2 进行数据加密传输，传输过程中节点数据安全系数在 0.4~0.6 之间，安全性中等。综合上述实验，得到如下所示的结论：相比传统方法，本文设计的基于 RSA 算法的数据加密传输方法应用效果良好，该方法可以提高数据加密传输过程中，无线异构通信网络节点的安全系数，通过此种方式，为移动通信过程中的数据安全提供进一步的保障。

5 结语

为解决数据在传输中存在的多种隐患问题，提高数据传输安全性与可靠性，本文引进RSA算法，以无线异构通信网络为例，对数据加密传输方法展开了设计研究。通过对比实验证明了该方法可以提高数据加密传输过程中，无线异构通信网络节点的安全系数。

参考文献：

[1] 刘张榕，余根坚. 融合 Ethereum 和 IPFS 加密算法的分布式数据存储传输研究 [J]. 佳木斯大学学报 (自然科学版)，2022,40(06):47-50+133.
[2] 张乐.基于 DES 和 RSA 加密技术的大数据加密传输技术的算法研究[J].无线互联科技,2022,19(18):125-127.
[3] 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),2022,34(15):224-228.
[4] 时春波，李卫东，秦丹阳，等.Python 环境下利用 Selenium 与 JavaScript 逆向技术爬虫研究[J].河南科技,2022,41(10):20-23.
[5] 范海涛，张宁.基于日志解析的网络数据传输信息安全自动加密系统优化[J].自动化技术与应用,2022,41(04):58-62.
[6] 邹洪,刘家豪,陈锋,等.基于递归神经网络的原始训练数据防泄漏密码生成系统设计[J].电子设计工程,2022,30(05):122-126.
[7] 李海勇,田君杨,曾令森,等.基于录波器合规并网的数据分层治理和安全防护架构设计 [J]. 电力信息与通信技术,2022,20(01):92-99.
[8] 徐伟，危蓉. 基于消息队列遥测传输和椭圆曲线加密的物联网身份验证方案[J].厦门大学学报(自然科学版),2021,60(06):1024-1031.
[9] 梁华. 电力系统在线监测装置无线传输网络安全分区改造的实施与应用[J]. 机电信息,2021,(09):1-2.
[10] 陈春妙,余佳熹,韦登帅,等.大数据背景下用户隐私安全保护研究——以 Android 应用为例[J].信息与电脑(理论版),2021,33(02):200-202.
[11] 谷正川,郭渊博,方晨.基于代理重加密的消息队列遥测传输协议端到端安全解决方案[J].计算机应用,2021,41(05):1378-1385.