 DOI: https://doi.org/10.12349/iser.v5i10.3483

Application of Data Communication Security Technology in Mobile Internet Environment

Bolin Li

Qingdao Agricultural University, Qingdao, Shandong, 265400, China

Abstract

In today's era, network technology has penetrated into all walks of life, and the penetration rate of portable smart devices continues to rise. From this point of view, People's Daily life and social progress have enjoyed a certain degree of convenience. However, in the field of data transmission security, we still face many challenges, such as data leaks and malicious tampering incidents occur frequently. In view of this, the relevant institutions must quickly conduct in-depth research on the security of servers and intelligent devices in the mobile network environment, and take the initiative to develop a more scientific network security communication scheme. At the same time, it is necessary to fully consider the unique attributes of the Internet. After specialized detailed analysis and research, technical innovation schemes such as elliptic curve encryption have been gradually formed, which greatly enhance security. Through these measures, the integrity and security of servers and smart devices can be effectively guaranteed. Based on this, this paper mainly analyzes the specific application of security technology in data communication under the mobile Internet environment, in order to provide reference and reference for the same industry personnel.

Keywords

mobile Internet; data communication security technology; apply

移动互联环境下数据通信安全技术的应用微探

李柏霖

青岛农业大学，中国 · 山东 青岛 265400

摘　要

在现今时代，网络技术已经渗透到各行各业，而便携式智能设备的普及率也在持续攀升。由此看来，民众的日常生活和社会进步都享受到了一定的便捷性。然而，在数据传输安全领域，我们依然面临着众多挑战，诸如数据泄露和恶意篡改事件频繁出现。鉴于此，有关机构必须迅速对移动网络环境下的服务器及智能设备安全进行深入的研究，主动制定更为科学的网络安全通信方案。同时，还需充分考虑到互联网的独有属性。经过专业化的详细分析和研究，逐步形成了椭圆曲线加密等技术创新方案，这些方案大大增强了安全性。通过这些措施，能够有效保障服务器和智能设备的完整性与安全防护。基于此，论文主要就移动互联环境下安全技术在数据通信中的具体应用进行分析，以期为同行业人员提供参考和借鉴。

关键词

移动互联；数据通信安全技术；应用

1 引言

在当今社会，手机这一移动设备已经成为人们生活中不可或缺的一部分，它极大地简化了我们的日常琐事和工作流程。然而，它犹如一把锋利的剑，既带来了方便，也潜藏着风险。移动设备让信息交流变得更加便捷，但同时也让信息泄露和盗窃变得易如反掌。由于网络环境的错综复杂，数据在传输过程中的安全面临着严峻挑战，数据被篡改或窃取的风险居高不下。因此，探索如何有效确保数据的安全性和完整性，是现阶段亟待解决的课题。

【作者简介】李柏霖（2003–），男，中国山东烟台人，本科，从事移动互联研究。

2 移动互联环境下数据通信的安全问题分析

随着移动网络技术深入我们的日常生活，它已经成为了推动社会向前发展的关键力量。它不仅深刻地改变了人们的日常生活习惯，还在人际交流、职场作业以及休闲娱乐等方面带来了革命性的变化。然而，尽管如此，移动网络技术也伴随着一些不足之处，比如安全隐患的层出不穷，以及对于安全技术进步的种种限制。鉴于此，对移动网络技术相关的安全风险进行深入探讨显得尤为迫切和重要。

首先，在移动互联网领域，随着数据传输和移动网络技术的融合，IP 地址的共享现象日益增多，这虽然为大众带来了极大的便利，但也给病毒入侵开启了方便之门。公共 Wi-Fi 网络作为移动互联的重要组成部分，其安全性问题尤为突出。攻击者可能利用公共 Wi-Fi 网络的漏洞，窃取用户的敏感信息，如账号密码、支付信息等。伴随着移动网络

技术的广泛应用，系统本身暴露出诸多弱点，这些弱点使得黑客能够对移动互联网进行全面扫描，寻找安全漏洞，从而严重威胁了数据传输的安全，这对移动网络技术的长远发展构成了不利影响。其次，在移动网络环境中，保障数据传输的安全性依赖于智能手机的作用至关重要。基于此，不法分子常常针对用户的手机发起攻击，比如随意破坏、严密监控以及非法获利，这些行为严重威胁到了用户的财产安全。除此之外，手机恶意软件种类繁多。例如，有的软件能够窃取用户的通话和短信信息，或是追踪手机位置，进而掌握用户的地理位置信息，对用户的财产安全构成威胁。最后，相较于传统手段，当代移动数据防护技术所涵盖的范畴与实施手段更为丰富，其隐秘性不断增强，安全隐患亦趋严峻。涉及数据传输互联的所有用户群体，包括但不限于通信服务商、硬件生产商以及软件开发者，都将面临潜在威胁。研究传播途径的成果显示，恶意软件不仅能够通过信息及邮件进行扩散，还能够直接内置于手机的核心部件。最为令人忧虑的是，这些病毒能够通过网络及蓝牙技术传播，对智能手机的正常运作构成威胁。总而言之，这些安全威胁的波及范围极其广泛，因此有关单位必须加大研究力度，寻求解决之道，为消除这些潜藏的安全隐患打下坚实的根基。

3 移动互联环境下数据通信安全技术的应用方案

论文融合了网络领域内已相对成熟的技术手段，并针对移动网络特性，深入研究了移动网络环境下的数据传输安全方案。在移动网络数据交换过程中，对涉及隐私的信息通过椭圆曲线加密技术进行安全加密，而对于那些非关键且不涉及隐私的数据则直接以明文形式传输。此方法不仅优化了数据处理与传输的效率，同时也确保了关键信息在移动网络交互过程中的安全。研究提出的方案整合了 SHA 算法、数字签名技术、椭圆曲线加密等多种技术，旨在确保 Android 智能设备应用程序与 Web 服务器在移动网络环境下的数据交换达到安全、完整、一致且不可否认的标准。为确保移动应用与服务器间数据交换的安全性，采纳椭圆曲线加密技术对敏感信息进行编码，以维护数据安全；运用 SHA 算法创建数据摘要，确保信息的完整性与一致性；并通过数字签名手段，保障信息的不可否认性。图 1 展示了从移动端至服务器的单向数据处理过程，而服务器至移动端的单向数据处理流程亦然。论文将依照图 1 所示方案，着重阐述从移动端至服务器单向数据的处理细节。

4 移动互联环境下数据通信安全策略中的关键技术

4.1 概述椭圆曲线密码体制

椭圆曲线密码体制本质上是通过有限域中椭圆曲线上的点集来实现离散对数加密方法。实际上，对椭圆曲线的离散对数进行计算是一项挑战性的任务。在椭圆曲线加密技术中，它能实现数据的加密处理，并在签名环节，确保安全通信过程中完成密钥交换。其计算负担轻、运行效率高和存储空间占用小等优势，使其在智能设备上应用更为便捷。通过将 ECC 与 RSA 加密体系进行对比分析，我们可以明显看出二者之间的差异。在相同的安全级别下，ECC 所需的密钥长度更短。而在密钥生成或验证过程中，ECC 的效率也更为突出。

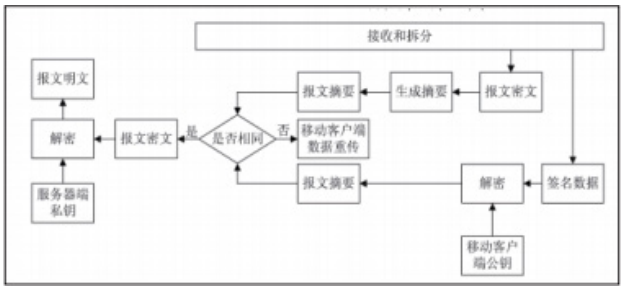

图 1 手机端访问服务器单向通信安全设计方案

4.2 数字签名

数字签名算法融合了非对称加密与哈希摘要技术，主要作用在于确认信息内容的完整性和来源的真实性，同时保证信息发送的行为无可否认。在这一技术中，哈希摘要技术是不可或缺的一环，它负责对信息完整性的检验。数字签名由生成和验证两个步骤构成，而在这些步骤中，技术人员通常使用 ECDSA 方法。ECDSA 是基于椭圆曲线加密 ECC 和数字签名算法 DSA 的融合，以其快速的处理速度、强大的安全性能和较短的签名长度而著称。根据所采用的摘要算法差异，数字签名算法主要可分为 MD5 和 SHA 两大流派，例如无摘要的 ECDSA、SHA1 与 ECDSA 结合、SHA256 与 ECDSA 结合以及 SHA512 与 ECDSA 结合等。论文所提及的方案，选用的是 JDK8 内置的 Signature 抽象类所支持的 SHA1 with ECDSA 算法，其依赖的消息摘要算法为 SHA1。

4.3 信息摘要算法

在执行信息摘要处理的过程中，信息的完整性与一致性均能够得到有效的维护。一般来讲，每个文件都会具备独特的“数字标识”，这样便可以形成数字签名的功能。如果文件内容发生了变动，原先的信息摘要也会随之出现变化。目前，广泛使用的信息摘要方法包括 MD5 和 SHA1。这两种方法都是基于散列函数构建的，且具备单向加密的特性。相比之下，SHA1 在抵御攻击方面的能力更强，因而其应用效果更为显著。

4.4 Bouncy Castle 与 Spongy Castle

在论文所提出的方案中，无论是加密还是解密环节，均采纳了椭圆曲线加密技术，具体应用的是椭圆曲线集成加密标准 ECIES。尽管 JDK8 原本支持的加密算法列表中包含 ECIES，但实际上默认安装的 JDK8 版本并没有包含支持此算法的提供者。因此，必须引入一个外部的提供者以支持该算法。所谓的提供者，是指那些实现了 Java 安全框架中部分或全部安全相关接口的类。Bouncy Castle 库正是这样一个提供了轻量级密码学 API 的第三方库，它作为 Java 加密扩展（JCE）的一个提供者，支持多种加密功能。在网页服务器的编程过程中，涉及密钥对生成以及加密、解密功能时，采用了 Bouncy Castle 加密库作为 Provider。然而，因为

Android 系统预装了一个经过简化的 Bouncy Castle 早期版本，导致在 Android 设备上引入 Bouncy Castle 的最新版本时，常常会遇到类加载的冲突问题。针对这一问题，Spongy Castle 对 Bouncy Castle 进行了调整优化，确保了其在 Android 平台上的兼容性。因此，针对 Android 客户端的密钥对生成及加密、解密功能，采用的是 Spongy Castle 加密库。

5 移动互联环境下数据通信安全技术的实现过程

论文从移动通信数据的不同展现层面，如网络终端服务器端、第三方加密库 Bouncy Castle 以及 Android 应用程序等方面，深入剖析了在互联网技术背景下数据通信安全技术的应用。在 Android 应用的数据传输环节，往往涉及到敏感信息的传递，这些信息必须通过密钥加密手段来保护，而对于关键数据，则需采用端到端的加密措施，确保信息在发送至接收的整个流程中保持加密状态，无需任何解密操作。开发者需重视数据的保密性，高效利用资源并保障数据处理的速度。只有在数据匹配确认无误后，才能继续后续操作，以获取所需信息。在此过程中，公私钥对的生成是关键环节，以 Bouncy Castle 加密算法为例，要求服务器端使用一致且唯一的密钥对。服务器会自动存储私钥密码，而公钥则部署到 Android 应用的程序中，使得用户能够获取公钥，进而解密得到所需的文本和视频等信息。目前，Android 系统的手机在数据传输方面采用的是在特定服务器上生成的一对匹配的公私钥。以下是详细的接收过程说明：首先，通过手机与服务器之间的公钥，生成移动设备接收端的公钥，进而采用椭圆曲线加密技术对敏感数据进行加密，这正是我们之前所讨论的加密手段。在数据传输阶段，通过 SHA 算法生成数据的摘要。数据接收方需进行数字签名验证和密文解密。预计未来这一系列流程将向智能化方向转变。公钥主要担当数据解密的角色，它独立存在，并不对数据传输造成影响。通过对摘要信息进行细致分析，可以及时识别出不一致的报文，从而在移动通信中发现问题，并确保最终获取正确的解密数据。

6 移动互联环境下数据通信安全技术应用的保障措施

6.1 经常性的安全性评估

在常规情境下，数据传输网络通常是指企业或机构内部搭建的一种网络体系，它既能实现组织内部的信息交流，又能与外部广阔的网络世界相连。为了保障网络环境的安全，必须在其运行过程中不断开展网络安全的评价工作。这种网络安全评价，针对的是局域范围内的数据传输网络，通过审查过程来判断网络系统内部是否潜藏安全风险，并测定网络的安全等级，以便对网络维护提供指导。进行网络安全评价的操作，通常由专业的网络维护团队负责，他们对网络安保设施的软硬件性能指标进行检测与评估。通过这种详尽的评价活动，可以有效地识别并掌握网络安全中潜在的风险点，从而降低网络运行过程中出现安全问题的概率。

6.2 及时消除网络漏洞与安全威胁

在识别出网络安全隐患和威胁之后，针对数据传输网络开展专门的维护作业和应对措施之外，更要全面强化其整体安全防护能力。起初，针对网络漏洞和安全风险的清除，需要利用服务器对网络数据进行深入分析，以便发现具体的安全缺陷并加以修复；面对病毒侵袭的威胁，可以通过安装防病毒软件来进行检测和防护，或是部署防火墙以有效阻挡病毒入侵，如在防火墙设置中对网络接口进行管控，审核通过防火墙的数据传输，防止不安全的网络应用扩散，对数据通信网络安全构成威胁。同时，还应定期更新防火墙的软件版本。其次，为了全面提升网络的安全防护级别，以下措施必不可少：一是定期清除网络环境中可能潜藏的安全风险软件及文档，并对可能藏有病毒的网址链接实施访问控制；二是不断对网络硬件设施进行更新换代，以增强网络的稳健性；三是企业宜采用外包手段，将核心主机系统与服务器分离，并在关键时候将内部网络与外部网络实行物理隔绝，这样方可有效防止病毒通过外部设备侵袭服务器，进而显著降低因网络安全缺陷带来的损失。

6.3 谨慎注意外部设备接入内网

以本地服务器运行的内网服务器，应使用白名单的设备或者使用自身的定制的操作系统保证安全，对违规外联行为及网络边界点的实时发现和处置，避免信息泄露或重要文件区被其他非特定权限者访问。个人设备在外部网络环境中易受病毒感染。移动设备的操作系统是设备的核心，一旦存在安全漏洞，就可能被攻击者利用进行非法操作，进而危及内网服务器，对服务器存储的数据造成破坏。需要对接入服务器或在计算机上存储、处理敏感信息文件的敏感操作实时发现和处置。

7 结语

随着中国科技实力的稳步攀升，相关部门愈发注重在移动互联网领域应用数据通信安全技术。期望通过这项技术的推广，显著增强中国移动互联网的安全防护能力，这对于改善网络环境同样具有至关重要的价值。当前，中国正站在移动网络环境发展的转折点上，信息以云的形式存储在网络，各行各业的大量重要数据在网络中存储传递，在这一关键时刻，深入探讨移动通信的安全性成为当下的核心任务，亦是行业长远发展的核心技术需求和关键所在。相关从业者需结合研究进展，全力以赴推进这一领域的工作，确保移动互联网中的数据通信安全得以实现。

参考文献

[1] 马赞.移动互联环境下数据通信安全技术的应用研究[J].中国新通信,2018(8):108.

[2] 林素珍.初探移动互联下的数据通信安全技术应用[J].通讯世界,2017(4):104-106.

[3] 周卫宁,刘友刚.移动互联网发展技术与安全问题[J].科技传播,2015(3):239+252.

[4] 白永祥.基于ECDSA的智能卡软件设计与实现[J].电子设计工程,2015,23(14):29-32.

[5] 范云海.集成加密方案ECIES的设计与验证[J].信息技术,2012(1):115-117.