Computer Science and Application 计算机科学与应用, 2021, 11(9), 2280-2288
Published Online September 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.119233

Hans汉斯

面向数字版权管理系统的轻量级三因素认证方案的分析与改进

麦凯强，亢保元，李　蕊

天津工业大学计算机科学与技术学院，天津
Email: 337167647@qq.com, baoyuankang@aliyun.com, 1103814823@qq.com

收稿日期：2021年8月13日；录用日期：2021年9月10日；发布日期：2021年9月17日

摘　要

随着嵌入式技术和低功耗设备的发展，数字内容开始在物联网、智能家居、车联网等各种资源有限的环境中进行传输和存储。但是，在公开信道上数字内容很容易被复制和分发，这使数字内容的提供者和合法的使用者的权益遭受严重的安全威胁。为了保护与数字内容相关参与者的合法权利，数字版权管理系统应运而生。2020年，Yu等人提出了一个基于生物特征的数字版权管理系统认证方案。本文对其进行了安全分析，发现Yu等人的方案不能正常运行并且容易受到用户的跟踪攻击和假冒许可服务器攻击。为了克服Yu等人方案的安全缺陷，本文提出了一个改进的面向数字版权管理系统的三因素认证方案，分析了它的安全性，并比较了它与同类方案的计算成本。

关键词

数字版权管理系统，认证方案，安全性

Analysis and Improvement on a Lightweight Three-Factor Authentication Scheme for Digital Rights Management System

Kaiqiang Mai, Baoyuan Kang, Rui Li

School of Computer Science and Technology, Tiangong University, Tianjin
Email: 337167647@qq.com, baoyuankang@aliyun.com, 1103814823@qq.com

Received: Aug. 13th, 2021; accepted: Sep. 10th, 2021; published: Sep. 17th, 2021

文章引用: 麦凯强, 亢保元, 李蕊. 面向数字版权管理系统的轻量级三因素认证方案的分析与改进[J]. 计算机科学与应用, 2021, 11(9): 2280-2288. DOI: 10.12677/csa.2021.119233

Abstract

With the development of embedded technology and low-power devices, digital content has begun to be transmitted and stored in various resource-limited environments such as the Internet of Things, smart homes, and Internet of Vehicles. However, digital content is easily copied and distributed on open channels, which causes serious security threats to the rights and interests of digital content providers and legitimate users. In order to protect the legal rights of participants related to digital content, a digital rights management system came into being. In 2020, Yu *et al.* proposed a biometric-based digital rights management system authentication scheme. This article conducted a security analysis on it and found that the scheme of Yu *et al.* does not work properly and is vulnerable to user tracking attacks and licensing server fake attacks. In order to overcome the security flaws of Yu *et al.*'s scheme, this paper proposes an improved three-factor authentication scheme for digital rights management system, analyzes its security, and compares its computational cost with similar schemes.

Keywords

Digital Rights Management System, Authentication Scheme, Safety

1. 引言

随着数字化和网络化的发展，数字内容的管理变得越来越复杂。由于数字内容在公开信道上传输和存储时容易被复制和分发，从而让侵犯版权行为日益增多。非法下载给版权提供者和合法所有者在各个方面都造成了巨大的损失。因此，数字版权管理系统对于保护版权提供者和合法所有者的权利及利益起到了至关重要的作用。

此外，数字内容服务也容易受到恶意攻击者的潜在攻击。因此，当所提供的数字内容服务变得多样时，数字版权管理系统也需要具备更加安全和高效的技术。数字版权管理系统的用户认证和密钥协商机制逐渐成为了向合法用户提供安全服务的基本需求。对于安全性的其他需求，数字版权管理系统还必须提高对数字内容的保密性并加强对数字内容的安全访问控制。另一方面，由于数字版权管理系统的智能设备资源有限，所以，用于数字版权管理系统的认证方案必须尽可能地降低计算和通信成本。2020 年，Yu 等人[1]发现 Lee 等人[2]的方案容易受到移动设备盗窃的攻击和攻击者假冒用户的攻击，并提出了一个基于生物特征的数字版权管理系统轻量级三因素认证方案。但在本文中，我们发现 Yu 等人的方案[1]并不能正常的运行，也无法抵抗用户的跟踪攻击以及用户的假冒攻击，且不能确保安全的相互认证。因此，本文先对 Yu 等人的方案[1]进行分析，然后指出其漏洞并进行改进，设计了一个改进的面向数字版权管理系统的轻量级三因素认证方案，并分析了改进方案的安全性。同时还参考了其他相关的认证方案[3]-[10]。最后，将改进方案和 Lee 等人的方案[2]、Chang 等人的方案[11]、Mishra 等人的方案[10]的计算通信开销进行了比较。

本文的其余部分组织如下：第 2 节介绍了相关的网络模型和数字版权管理系统。第 3 节和第 4 节回顾了 Yu 等人[1]的数字版权管理系统认证方案，并进行了安全性分析。第 5 节提出了一个改进的数字版

权管理系统的认证方案。第 6 节对新提出的方案进行了安全分析，以及计算通信开销的分析比较。最后，第 7 节给出了本文的结论。

2. 网络模型

由于在公开信道上数字内容很容易被复制和分发，因此通过数字版权管理技术保护数字内容尤为重要。一个数字版权管理系统通常由用户、内容提供商、许可证服务器和内容服务器四个实体组成。

如图 1 所示，在创建数字内容时，内容提供商使用密钥对数字内容进行加密，并通过安全信道将加密数字内容的密钥传输到许可证服务器，同时通过 VPN 通道将加密的数字内容发送到内容服务器。内容服务器在接收到加密的数字内容后将其存储在数据库中，许可证服务器在接收到密钥后也将其存储在它的数据库中。当用户请求加密数字内容的密钥时，许可服务器首先验证用户的合法性。一旦用户和许可服务器成功地实现相互认证，用户就可以获得加密数字内容的密钥，从而实现对数字内容的访问。

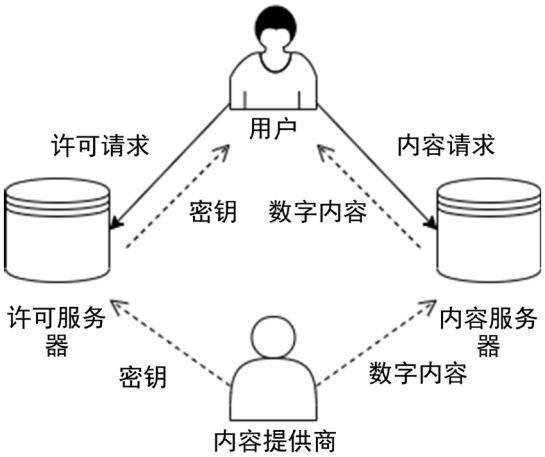

Figure 1. Digital rights management system
图 1. 数字版权管理系统

3. Yu 等人方案的回顾

本节回顾了 Yu 等人[1]在 2020 年提出的适用于数字版权管理系统的安全认证和密钥分配方案。Yu 等人的方案包含三个阶段：注册阶段、登录和身份验证阶段以及口令更新阶段。但限于篇幅，本节省略与文本关联不大的口令更新阶段，仅回顾前两个阶段。由于 Yu 等人的方案[1]仅实现了用户 U_i 和许可服务器 S_j 这两个实体的相互认证，且与内容服务器和内容提供商这两个实体无关。因此，Yu 等人的方案[1]及本文的改进方案不会涉及内容服务器和内容提供商这两个实体。本文所用到的符号及意义如表 1 所示。

Table 1. Symbols and meanings used in this article
表 1. 本文用到的符号及意义

符号	意义
U_i	用户
PW_i	用户 U_i 的口令
ID_i	用户 U_i 的身份标识
BIO_i	生物特征
S_j	许可服务器

Continued

ID_{DC} 数字内容的身份标识
R_1 用户 U_i 选取的随机数
R_2 许可服务器 S_j 选取的随机数
X_s 许可服务器 S_j 的密钥
KEY_{DC} 数字内容的密钥
a_u, a_u^{new} 用户 U_i 的选取的随机数和用户 U_i 选取用于更新的随机数
ΔT 允许的最大延迟
$h(.)$ 单向哈希函数
$H(.)$ 生物哈希函数
$\oplus$ 按位异或运算
$\|$ 串联操作

3.1. 用户注册阶段

寻求访问数字内容服务的新移动用户 U_i 必须在许可证服务器 S_j 中注册其身份。 用户 U_i 通过以下步骤完成在许可证服务器 S_j 处的注册：

1) U_i 选取身份标识 ID_i 和口令 PW_i 并提取生物特征 BIO_i，通过模糊提取技术得到 $Gen(BIO_i)=\langle R_i, P_i\rangle$，计算 $RPW_i = h(PW_i \| R_i)$，然后将 $\{ID_i, RPW_i\}$ 通过安全的信道发送给许可证服务器 S_j。

2) S_j 接收到来自 U_i 发送的 $\{ID_i, RPW_i\}$ 后，计算 $X_i = h(ID_i \| X_S)$，$d_i = X_i \oplus h(ID_i \| RPW_i)$，$f_i = h(RPW_i \| X_i)$。然后，$S_j$ 将 ID_i 和 X_i 一起存储到数据库中并将 $\{d_i, f_i\}$ 通过安全的信道发送给 U_i。

3) U_i 接收到来自 S_j 发送的 $\{d_i, f_i\}$ 后，将 $\{d_i, f_i\}$ 存储到设备中。

3.2. 登录和认证阶段

注册完成后，用户 U_i 向许可证服务器 S_j 发送登录请求消息。这个阶段的目标是实现 U_i 和 S_j 的相互认证，然后 S_j 将数字内容的密钥分发给 U_i。此阶段通过以下几个步骤完成：

1) 用户 U_i 输入 ID_i、PW_i 和 BIO_i 到设备中，设备恢复 $R_i = Rep(BIO_i, P_i)$，计算 $RPW_i = h(PW_i \| R_i)$，$X_i = d_i \oplus h(ID_i \| RPW_i)$ 和 $f_i^* = h(RPW_i \| X_i)$，并比较得出的 f_i^* 与设备中所存储的 f_i 是否相等。若相等，设备生成随机数 R_1 并计算 $M_1 = X_i \oplus R_1$，$M_2 = ID_i \oplus R_1$，$M_3 = ID_{DC} \oplus R_1$ 和 $M_{US} = h(ID_i \| ID_{DC} \| X_i \| R_1)$。然后，$U_i$ 将消息 $\{M_1, M_2, M_3, M_{US}\}$ 发送给许可服务器 S_j。

2) S_j 收到来自 U_i 的消息 $\{M_1, M_2, M_3, M_{US}\}$ 后，计算 $R_1 = M_1 \oplus X_i$，$ID_i = M_2 \oplus R_1$，$ID_{DC} = M_3 \oplus R_1$ 和 $M_{US}^* = h(ID_i \| ID_{DC} \| X_i \| R_1)$。然后，检测 $M_{US}^* = M_{US}$ 是否成立，若成立，S_j 生成随机数 R_2，计算 $M_4 = R_2 \oplus X_i$，$M_5 = KEY_{DC} \oplus X_i$ 和 $M_{SU} = h(ID_i \| X_i \| KEY_{DC} \| R_2)$。最后，$S_j$ 将消息 $\{M_4, M_5, M_{SU}\}$ 发送给 U_i。

3) U_i 收到来自 S_j 的消息 $\{M_4, M_5, M_{SU}\}$ 后，计算 $R_2 = M_4 \oplus X_i$，$KEY_{DC} = M_5 \oplus X_i$ 和 $M_{SU}^* = h(ID_i \| X_i \| KEY_{DC} \| R_2)$。最后，$U_i$ 验证 M_{SU}^* 与 M_{SU} 是否相等。若相等，则将 KEY_{DC} 存储到设备中。

4. Yu 等人方案的安全性

本节分析 Yu 等人方案[1]的安全性。分析结果表明，该方案无法正常的运行。此外，该方案还不能抵抗对用户的跟踪攻击以及对许可服务器的假冒攻击。

4.1. Yu 等人的方案无法正常运行

在登录与认证阶段的第一步，由于用户U_i向许可服务器S_j发送的消息$\{M_1, M_2, M_3, M_{US}\}$中缺少用户$U_i$的身份信息，导致 Yu 等人方案[1]无法正常运行。当用户U_i将消息$\{M_1, M_2, M_3, M_{US}\}$发送给许可服务器$S_j$后，$S_j$计算$R_1 = M_1 \oplus X_i$。然而，在用户注册阶段中，$S_j$将$X_i$和$ID_i$一起存储在数据库中。于是，$S_j$要找到$X_i$，必须要求$U_i$提供其身份信息。而在$U_i$向$S_j$发送的消息$\{M_1, M_2, M_3, M_{US}\}$中显然缺少$U_i$的身份信息$ID_i$。因此，$S_j$不能找到对应的$X_i$来计算$R_1 = M_1 \oplus X_i$。从而，$S_j$无法计算$R_1 = M_1 \oplus X_i$，该方案无法正常的运行。

4.2. 跟踪攻击

在 Yu 等人方案[1]的登录和认证阶段，攻击者 A 截获用户U_i向许可服务器S_j发送消息$\{M_1, M_2, M_3, M_{US}\}$后，可以进行如下的跟踪攻击：

攻击者 A 首先计算$M_1 \oplus M_2 = X_i \oplus ID_i$。由于等式右边的$X_i$和$ID_i$均不变，因此$M_1 \oplus M_2$对用户$U_i$来说是一个不变的值。于是，攻击者 A 可以通过计算$M_1 \oplus M_2$来实现对用户U_i的跟踪。

4.3. 假冒许可服务器攻击

在 4.2 节跟踪攻击的基础上，攻击者 A 可以进行假冒许可服务器的攻击。具体来讲，当用户U_i在与许可服务器S_j联系并获得数字内容 DC 的密钥KEY_{DC}时，攻击者 A 可截获消息$\{M_1, M_2, M_3, M_{US}\}$和$\{M_4, M_5, M_{SU}\}$。此后，当攻击者 A 跟踪到用户$U_i$在寻求获得另一数字内容 dc 的密钥$KEY_{dc}$而与许可服务器$S_j$再次联系时，攻击者 A 可以假冒许可服务器$S_j$将上一次所截获的由$S_j$发送给$U_i$的消息$\{M_4, M_5, M_{SU}\}$直接发送给$U_i$。$U_i$在收到来自攻击者 A 发送的消息$\{M_4, M_5, M_{SU}\}$后，显然这个消息可以通过$U_i$的验证，并使$U_i$得到密钥$KEY_{DC}$，但这显然不是$U_i$寻求的数字内容 dc 的密钥$KEY_{dc}$。于是，攻击者假冒许可服务器的攻击获得成功。

5. 改进方案

为了克服 Yu 等人方案[1]所存在的安全缺陷，本文在增加动态身份、时间戳作为附加安全因素的基础上，提出了一个改进的面向数字版权管理系统的轻量级三因素认证方案。改进的方案包括两个阶段，分别是用户注册阶段以及登录和认证阶段，具体方案如下。

5.1. 用户注册阶段

用户U_i通过下列步骤完成在许可证服务器S_j处的注册。

1) U_i选取身份标识ID_i和口令PW_i，然后提取生物特征BIO_i，通过模糊提取技术得到$Gen(BIO_i) = \langle R_i, P_i \rangle$，计算$RPW_i = h(PW_i \| R_i)$。$U_i$生成随机数$a_i$并计算$DID_i = h(ID_i \| a_i)$，然后将$\{ID_i, RPW_i, DID_i\}$通过安全的信道发送给许可证服务器$S_j$。

2) S_j接收到$\{ID_i, RPW_i, DID_i\}$后，计算$X_i = h(ID_i \| X_S)$，$d_i = X_i \oplus h(ID_i \| RPW_i)$，$f_i = h(RPW_i \| X_i)$。执行计算后，$S_j$将动态身份$DID_i$和$X_i$一起存储到数据库中并将$\{d_i, f_i\}$通过安全的信道发送给$U_i$。

3) U_i接收到来自S_j发送的$\{d_i, f_i\}$后，将$\{d_i, f_i, a_i, P_i\}$存储到设备当中。

5.2. 登录和认证阶段

用户U_i通过下列步骤向许可证服务器S_j发送登录请求消息，实现相互认证，并最终获得由S_j发送过来的数字内容 DC 的密钥KEY_{DC}。

1) 用户 U_i 输入 ID_i、PW_i 并扫描 BIO_i 到设备中，设备通过模糊识别技术恢复 $R_i = Rep(BIO_i, P_i)$，并计算 $RPW_i = h(PW_i \| R_i)$，$X_i = d_i \oplus h(ID_i \| RPW_i)$ 和 $f_i^* = h(RPW_i \| X_i)$ 然后比较得出的 f_i^* 与设备中所存储的 f_i 是否相等。若相等，设备生成随机数 R_1 和 a_i^{new} 并获取当前时间戳 T_1。然后计算 $DID_i = h(ID_i \| a_i)$，$DID_i^{new} = h(ID_i \| X_i \| a_i^{new})$，$M_1 = X_i \oplus R_1$，$M_2 = DID_i^{new} \oplus h(R_1)$，$M_3 = ID_{DC} \oplus h(h(R_1))$ 和 $M_{US} = h(DID_i \| ID_{DC} \| X_i \| R_1 \| T_1)$。最后，$U_i$ 将随机数 a_i 更新为 a_i^{new} 并存储到设备中，然后将消息 $\{M_1, M_2, M_3, M_{US}, DID_i, T_1\}$ 发送给许可服务器 S_j。

2) S_j 收到来自 U_i 的消息 $\{M_1, M_2, M_3, M_{US}, DID_i, T_1\}$ 后，获取当前时间戳 T_1'，验证 $|T_1' - T_1| \le \Delta T$，根据 DID_i 找到 X_i 并计算 $R_1 = M_1 \oplus X_i$，$DID_i^{new} = M_2 \oplus h(R_1)$，$ID_{DC} = M_3 \oplus h(h(R_1))$ 和 $M_{US}^* = h(DID_i \| ID_{DC} \| X_i \| R_1 \| T_1)$ 并比较得出的 M_{US}^* 与 U_i 发送过来的 M_{US} 是否相等。若相等，S_j 成功认证 U_i。然后，S_j 生成随机数 R_2 并获取当前时间戳 T_2，计算 $M_4 = R_2 \oplus X_i$，$M_5 = KEY_{DC} \oplus h(X_i)$，$M_6 = DID_i^{new} \oplus h(h(X_i))$，$M_{SU} = h(DID_i^{new} \| X_i \| KEY_{DC} \| R_2 \| T_2)$。最后，$S_j$ 将动态身份 DID_i 更新为 DID_i^{new} 并和 X_i 一起存储到数据库中，然后将消息 $\{M_4, M_5, M_6, M_{SU}, T_2\}$ 发送给 U_i。

3) U_i 收到来自 S_j 的消息 $\{M_4, M_5, M_6, M_{SU}, T_2\}$ 后，获取当前时间戳 T_2'，验证 $|T_2' - T_2| \le \Delta T$，计算 $R_2 = M_4 \oplus X_i$，$KEY_{DC} = M_5 \oplus h(X_i)$，$DID_i^{new} = M_6 \oplus h(h(X_i))$ 和 $M_{SU}^* = h(DID_i^{new} \| X_i \| KEY_{DC} \| R_2 \| T_2)$。然后，$U_i$ 比较计算得到 M_{SU}^* 与 S_j 发来的 M_{SU} 是否相等。若相等 U_i 成功认证 S_j 并将获得的数字内容的密钥 KEY_{DC} 存储到设备中。

6. 改进方案的安全性分析

本阶段对所提出的改进方案进行安全分析。

6.1. 改进方案可以实现用户的不可跟踪性和匿名性

在本文的 4.2 节中提到对 Yu 等人方案[1]进行了跟踪攻击。其中，攻击者 A 可以通过截获用户 U_i 向许可服务器 S_j 发送的消息 $\{M_1, M_2, M_3, M_{US}\}$ 并计算 $M_1 \oplus M_2 = X_i \oplus ID_i$，由于其中 X_i 和 ID_i 均不变使得攻击者 A 可以对用户进行跟踪攻击。然而，改进的方案采用了动态身份来代替用户静态的身份，同时对消息 $M_2 = DID_i^{new} \oplus h(R_1)$，$M_3 = ID_{DC} \oplus h(h(R_1))$，$M_5 = KEY_{DC} \oplus h(X_i)$，$M_6 = DID_i^{new} \oplus h(h(X_i))$ 增加了单向散列函数的运算以防止通过计算 $M_1 \oplus M_2 = X_i \oplus ID_i$ 或者其他消息间进行两两的异或运算而得出关键信息。倘若在改进方案中对用户进行跟踪攻击，当攻击者 A 截获了消息 $\{M_1, M_2, M_3, M_{US}, DID_i, T_1\}$ 后。此时，攻击者 A 计算 $M_1 \oplus M_2 = X_i \oplus DID_i^{new} \oplus R_i \oplus h(R_i)$，其中的动态身份 $DID_i = h(ID_i \| a_i)$ 与用户选取的随机数 a_i 相关。然而，每次会话结束后 a_i 都会被用户 U_i 所更新，同时被更新的还有动态身份 DID_i^{new}。因此，在改进方案中，即便是同一用户在不同的会话中也有着不同的身份信息。通过以上分析，不难看出改进的方案实现了用户的不可跟踪性和匿名性。

6.2. 改进方案可以抵抗假冒许可服务器攻击

在本文的 4.3 节中提到对 Yu 等人方案[1]进行了假冒许可服务器攻击。其中，攻击者 A 需要先对用户进行跟踪攻击并截获消息 $\{M_1, M_2, M_3, M_{US}\}$ 和 $\{M_4, M_5, M_{SU}\}$。此后，当攻击者 A 跟踪到用户 U_i 在寻求获得另一数字内容的密钥而与许可服务器 S_j 再次联系时，攻击者 A 可以假冒许可服务器 S_j 将上一次所截获的由 S_j 发送给 U_i 的消息 $\{M_4, M_5, M_{SU}\}$ 直接发送给 U_i。此消息可以通过 U_i 的验证并使 U_i 得到密钥，但并不是 U_i 所寻求的数字内容的密钥。攻击者 A 由此可以进行假冒许可服务器攻击。然而，改进的方案中增加了时间戳。倘若攻击者想要成功实施假冒许可服务器攻击，其必须保证所截获的时间戳满足允许的最大延迟的验证。而攻击者是将上一次所截获的由 S_j 发送给 U_i 的消息 $\{M_4, M_5, M_{SU}\}$ 直接发送给 U_i，显然这无法满足验证的条件。因此，改进的方案可以抵抗假冒许可服务器攻击。

6.3. 改进方案可以实现用户和许可服务器的双向认证

在本文 5.2 节的 2)、3)中提到，用户 U_i 将消息 $\{M_1, M_2, M_3, M_{US}, DID_i, T_1\}$ 发送给许可服务器 S_j。S_j 首先检验 T_1 的有效性。然后，通过验证 M_{US}^* 与 U_i 发送过来的 M_{US} 是否相等来确认用户 U_i 的有效性。接下来，S_j 又将消息 $\{M_4, M_5, M_6, M_{SU}, T_2\}$ 发送给 U_i。U_i 也会先检验 T_2 的有效性，之后 U_i 通过验证 M_{SU}^* 与 S_j 发来的 M_{SU} 是否相等来验证 S_j 的合法性。因此，用户 U_i 和许可服务器 S_j 之间成功实现了双向认证。

6.4. 改进方案可以抵抗重放攻击

在改进的方案中，因为每次收到的消息都会用时戳进行验证，所以攻击者 A 无法进行重放攻击。例如，用户 U_i 在每次发送消息时都会加上当前时刻 T_i，许可服务器 S_j 在接收到消息后会根据当前时刻 T_i' 判断 $|T_i' - T_i| \le \Delta T$ 是否成立，如果成立，则继续对接收到的相关消息进行认证。当 U_i 收到 S_j 发送的消息后，会根据当前时刻 T_j' 判断 $|T_j' - T_j| \le \Delta T$ 是否成立，如果成立，才能执行其他计算。

6.5. 改进方案的性能分析

在这里，我们分别从计算开销和安全属性两方面分析了 Yu 等人的方案[1]、Lee 等人的方案[2]、Chang 等人的方案[11]、Mishra 等人的方案[10]和本文改进方案的性能。计算开销的对比及安全属性的对比分别如表 2、表 3 所示。为了方便讨论，用 T_h 表示单向散列函数的时间复杂度，T_x 表示异或运算的时间复杂度。运算耗费时间的顺序为：$T_h > T_x$。由表 2、表 3 可以看出改进方案的计算开销虽然相对比较高，但却实现了所有的安全属性。Yu 等人的方案[1]、Lee 等人的方案[2]、Chang 等人的方案[11]、Mishra 等人的方案[10]的总成本分别为 $11T_h + 12T_x$、$12T_h + 21T_x$、$14T_h + 14T_x$、$16T_h + 8T_x$。而改进方案的成本为 $26T_h + 14T_x$，虽然改进方案的计算成本略高于其他的方案，但 Yu 等人的方案[1]、Lee 等人的方案[6]、Chang 等人的方案[11]、Mishra 等人的方案[12]的方案容易受到以下所发起的各种攻击。同时，改进方案能够抵抗这些攻击。因此，改进方案相比其他方案要更加安全。

Table 2. Comparison of calculation efficiency of improvement schemes
表 2. 改进方案计算效率对比

方案	注册阶段登陆和认证阶段	总成本
Yu 等人的方案[1]	$4T_h + 1T_x$，$7T_h + 11T_x$	$11T_h + 12T_x$
Lee 等人的方案[2]	$3T_h + 4T_x$，$9T_h + 17T_x$	$12T_h + 21T_x$
Chang 等人的方案[11]	$2T_h + 2T_x$，$12T_h + 12T_x$	$14T_h + 14T_x$
Mishra 等人的方案[10]	$4T_h + 2T_x$，$12T_h + 6T_x$	$16T_h + 8T_x$
改进方案	$5T_h + 1T_x$，$21T_h + 13T_x$	$26T_h + 14T_x$

Table 3. Security comparison
表 3. 安全性对比

	Yu 等人的方案[1]	Lee 等人的方案[2]	Chang 等人的方案[11]	Mishra 等人的方案[10]	改进方案
相互认证	是	否	是	是	是
用户匿名性	是	是	是	否	是
移动设备丢失攻击	是	否	否	是	是

Continued

用户仿冒攻击	否	否	是	是	是
跟踪攻击	否	是	是	是	是
重放攻击	是	是	是	是	是
离线密码猜测攻击	是	是	否	是	是

7. 结论

在数字版权管理系统中，匿名性和不可追踪性非常重要，用户可以在不暴露自身身份且不被跟踪的情况下访问许可服务器并获取资源和数据。本文通过对 Yu 等人的方案[1]的安全分析发现 Yu 等人的方案[1]不能正常运行且容易受到用户的跟踪攻击和假冒许可服务器攻击。因此，本文对 Yu 等人[1]提出的基于生物特征的数字版权管理系统轻量级三因素认证方案进行改进，提出了一个改进的面向数字版权管理系统的轻量级三因素认证方案，以克服 Yu 等人方案[1]的安全缺陷。改进的方案不仅能够抵御用户的跟踪攻击、假冒许可服务器攻击和重放攻击，而且通过用存储在设备中的参数能够实现用户的身份匿名以及用户和许可服务器之间安全的相互认证。此外，本文还对改进方案进行了安全分析，同时还将改进方案与 Lee 等人的方案[2]、Chang 等人的方案[11]以及 Mishra 等人的方案的计算成本进行了比较。通过比较发现，改进方案显著地增加了安全性。但另一方面，改进方案为了提高安全性也增加了一定的计算开销。因此，需要通过对相关方案的学习研究[12] [13] [14] [15] [16]，在提升方案的效率和安全性同时减少计算开销的方面做进一步研究。

参考文献

[1] Yu, S.J., Park, K.S., Park, Y.H., Kim, H.P. and Park, Y.H. (2020) A Lightweight Three-Factor Authentication Protocol for Digital Rights Management System. *Peer-to-Peer Networking and Applications*, **13**, 1340-1356. https://doi.org/10.1007/s12083-019-00836-x

[2] Lee, C.C., Li, C.T., Chen, Z.W. and Lai, Y.M. (2018) A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System. *Information Technology and Control*, **47**, 262-274. https://doi.org/10.5755/j01.itc.47.2.18506

[3] Subramanya, S.R. and Yi, B.K. (2008) Digital Rights Management. *IEEE Potentials*, **25**, 31-34. https://doi.org/10.1109/MP.2006.1649008

[4] Chang, I.P., Lee, T.F., Lin, T.H. and Liu, C.M. (2015) Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. *Sensors*, **15**, 29841-29854. https://doi.org/10.3390/s151229767

[5] Das, A.K., Wazid, M., Kumar, N., Khan, M.K., Choo, K.K.R. and Park, Y. (2017) Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment. *IEEE Biomedical and Health Informatics*, **22**, 1310-1322. https://doi.org/10.1109/JBHI.2017.2753464

[6] Yu, S., Lee, J., Lee, K., Park, K. and Park, Y. (2018) Secure Authentication Protocol for Wireless Sensor Networks in Vehicular Communications. *Sensors*, **18**, 3191. https://doi.org/10.3390/s18103191

[7] Li, C.T. and Hwang, M.S. (2010) An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards. *Network and Computer Applications*, **33**, 1-5. https://doi.org/10.1016/j.jnca.2009.08.001

[8] Zhu, H. and Zhang, Y. (2017) An Efficient Chaotic Maps-Based Deniable Authentication Group Key Agreement Protocol. *Wireless Personal Communications*, **96**, 217-229. https://doi.org/10.1007/s11277-017-4163-x

[9] Wazid, M., Das, A.K., Kumari, S., Li, X. and Wu, F. (2016) Design of an Efficient and Provably Secure Anonymity Preserving Three-Factor User Authentication and Key Agreement Scheme for TMIS. *Secure Communication Network*, **9**, 1983-2001. https://doi.org/10.1002/sec.1452

[10] Mishra, D., Das, A.K. and Mukhopadhyay, S. (2015) An Anonymous and Secure Biometric-Based Enterprise Digital Rights Management System for Mobile Environment. *Secure Communication Network*, **8**, 3383-3404. https://doi.org/10.1002/sec.1266

[11] Chang, C.C., Chang, S.C. and Yang, J.H. (2013) A Practical Secure and Efficient Enterprise Digital Rights Manage-

ment Mechanism Suitable for Mobile Environment. *Secure Communication Network*, **6**, 972-984. https://doi.org/10.1002/sec.647

[12] Ali, Z., Ghani, A., Khan, I., Chaudhry, S.A., Islam, S.H. and Giri, D. (2020) A Robust Authentication and Access Control Protocol for Securing Wireless Healthcare Sensor Networks. *Journal of Information Security and Applications*, **52**, Article ID: 102502. https://doi.org/10.1016/j.jisa.2020.102502

[13] Aghili, S.F., Mala, H., Shojafar, M. and Peris-Lopez, P. (2019) LACO: Lightweight Three-Factor Authentication, AccessControl and Ownership Transfer Scheme for E-Health Systems in IoT. *Future Generation Computer Systems*, **96**, 410-424. https://doi.org/10.1016/j.future.2019.02.020

[14] 屈娟, 冯玉明, 李艳平, 李丽. 可证明安全的面向无线传感器网络的三因素认证及密钥协商方案[J]. 通信学报, 2018, 39(S2): 189-197.

[15] Chen, L. and Zhang, K. (2020) Privacy-Aware Smart Card Based Biometric Authentication Scheme for e-Health. *Peer-to-Peer Networking and Applications*, **2**, 1-13.

[16] Kumar, P. and Chouhan, L. (2021) A Privacy and Session Key Based Authentication Scheme for Medical IoT Networks. *Computer Communications*, **166**, 154-164. https://doi.org/10.1016/j.comcom.2020.11.017