doi:10.11959/j.issn.1000-436x.2017164

CASTWED：卫星移动通信系统中一种结合可穿戴设备与智能终端的持续认证方案

徐日新，陈小兵，祝烈煌
（北京理工大学计算机学院，北京 100081）

摘 要：智能手表、智能手环等各类可穿戴设备在世界范围内已经得到了迅猛发展。这些设备带有多种传感器，可以感知周围环境以及用户生物特征，同时可利用这些特征信息来持续认证持有智能终端的用户。然而，受限于卫星移动通信的低传输率以及身份认证过程中对于数据持续传输的需求，目前还没有在卫星移动通信系统中利用这些特征对用户进行持续身份认证的研究工作。为解决该问题，在卫星移动通信系统中，提出一个结合可穿戴设备与智能终端的持续认证方案（CASTWED），并对方案的安全性进行了理论分析。实验数据表明，CASTWED 方案可以在支持 10 万用户并发访问的同时，仅需占用 Ku 波段 60 Mbit/s 的传输带宽。

关键词：持续认证；智能终端；可穿戴设备；卫星移动通信
中图分类号：TP302 **文献标识码**：A

CASTWED: continuous authentication combining smart terminal with wearable devices in mobile satellite communication system

XU Ri-xin, CHEN Xiao-bing, ZHU Lie-huang
(School of Computer Science, Beijing Institute of Technology, Beijing 100081, China)

Abstract: Wearable devices, such as smart watches or smart bracelets, have been growing rapidly worldwide. These devices with various sensors have the ability to perceive the circumstance and user's biometric features, which can be used to continuously authenticate a user's identity. However, these features have not been studied to identify a specific user in mobile satellite communication system yet, due to its low data transfer rate and unacceptable delay. To solve this problem, continuous authentication combing smart terminal with wearable devices (CASTWED) was studied in mobile satellite communication system, the security of CASTWED was also theoretically analyzed. Simulation experiments show that the CASTWED scheme can provide simultaneous online authentication service for 100 000 users via 60 Mbit/s Ku wave band.

Key words: continuous authentication, smart terminal, wearable devices, mobile satellite communication

1 引言

随着网络的大规模部署以及各种应用场景，网络通信中对于用户的身份认证已经成为网络通信安全不可忽视的一个重要组成部分。很多特殊的场景涉及长时间的通信会话，为保证会话安全，需要持续性或周期性验证通信实体。考虑到便捷性和实用性，通信过程中的持续认证方案非常有必要。

自谷歌眼镜诞生后，各类智能手表、智能手环等可穿戴设备涌现出来[1]。美国 KPCB 风投认为在接下来的 10 年，可穿戴设备将会成为网络发展的一个重要环节[2]。这些可穿戴设备均带有多种传感器。例如，苹果智能手表中就具有陀螺仪、气压传感器、加速度传感器、红外传感器、光线传感器、心电监测传感器、脉搏氧饱和度传感器等 10 余种传感器。这些传感器间相互协同配合，实现监测用

收稿日期：2017-02-19；修回日期：2017-07-18
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2016YFB0800301）
Foundation Item: The National Basic Research Program of China (973 Program) (No.2016YFB0800301)

户周围环境信息以及用户身体特征的功能[3]。

目前，已经有研究者采用上述传感器采集数据数据，对用户身份进行认证[4~8]。考虑到这些传感器可以定期自动地采集数据，这种认证方式可实现持续性[5]。此外，由于这些传感器采集数据时无需用户进行任何额外的辅助操作，所以持续的身份认证过程还可以在后台隐式进行，无需打扰用户。虽然这个认证方案具有多种优势，但是，在卫星移动通信系统中实现持续认证方案还存在着许多研究空白。这一现状是由多种原因导致的。与天地一体化通信系统不同，传统网络通信场景缺少针对卫星通信系统的持续认证需求。且卫星通信链路带宽有限，在此种情况下，大规模实体持续认证需要对认证协议的设计提出很高的要求。

此外，学术界目前普遍关注的是可穿戴设备数据传输的低功耗或安全性。文献[9]提出了一种使用 NFC 的低功耗特性进行可穿戴设备认证的方法；文献[10,11]调研了目前可穿戴设备的通信方案并分析其安全性。由此可见，目前学术界对于大规模可穿戴设备与移动卫星之间的持续性身份认证方面研究较少，尚无成熟方案。

针对上述问题，本文提出一种结合可穿戴设备与智能终端的安全持续认证方案，系统模型如图 1 所示。该方案在认证过程中的通信开销小，处理速度快。通过模拟实验可知，该方案可以在 Ku 波段 60 Mbit/s 传输速率下，支持 10 万用户并发持续认证，具有一定的实用性。

2　相关工作

本节分别从可穿戴设备感知数据与身份认证，以及卫星移动通信网络中身份认证角度来介绍现有工作。

从利用可穿戴设备与智能终端感知数据和认证身份的角度，Porzi 等[5]利用智能手表持续认证方案。该方案利用加速度传感器和陀螺仪识别用户。Gafurov 等[6]利用加速度传感器，通过用户的步态来认证身份。Tijerina 等[7]提出了一个基于检测人体化学反应的用户身份认证方案。具体来说，通过设备发送无线信号后感知人体散发的气味来识别用户。Wong 等[8]采用智能终端中的扬声器和麦克风来检查人体中骨传导声音的差异，从而区分用户。

从卫星移动通信网络身份认证角度，李凤华等[12]指出了身份认证在卫星移动通信网络中扮演重要角色的观点。Gustafson 等[13]提出了一个基于密钥协商的卫星认证方案，利用设备间的相对位置，保证了认证的高效性。Chen 等[14]提出了一个基于口令的卫星认证方案，该方案通过加密和签名验证用户的身份，并保证消息的安全性。Lin[15]提出了一个无需认证表的动态卫星身份认证方案。该方案通过设计一个动态认证协议，使卫星无需使用认证表，提高了认证效率。Elmasri 等[16]把群组密钥管理方法引入到卫星身份认证方案中，提高了卫星认证协议的性能。

方案 1　基于口令的卫星移动通信认证方案

初始化阶段

指挥中心从阶为 q 的群 Z_p^* 中选择一个随机元素 x 作为私钥，并计算 $y = g^x \bmod p$ 作为公钥。

注册阶段

用户输入身份 U_{ID} 以及口令 pw 并计算 $w = h(U_{\mathrm{ID}}, pw)$ 最后发送 w 给指挥中心。

指挥中心选择一个临时身份 T_{ID} 和一个随机数 k 给用户，并计算签名 (r,s) 以及 b。其中，$r = g^k \bmod p$ ，$s = h(w)x + kr^{-1} \bmod q$ ，$b = h(s, x) \oplus w$。最后，指挥中心存储 $(T_{\mathrm{ID}}, r, s, b)$ 到认证表中，并发送给用户 (T_{ID}, r)。

认证阶段

用户输入身份 U_{ID} 和口令 pw，并计算 $w = h(U_{\mathrm{ID}}, pw)$、$sk = h(h(U_{\mathrm{ID}}, pw), T_{\mathrm{ID}})$、$c = MAC_{h(w,r)}(w, T_{\mathrm{ID}}, sk)$，

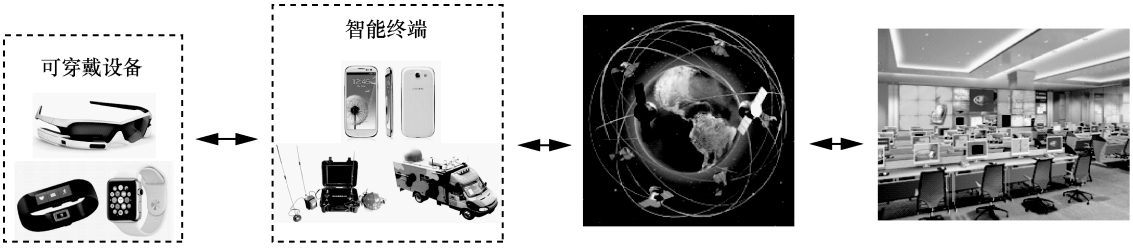


图 1　本文方案系统模型

用户发送 (T_{ID},c) 给指挥中心。

指挥中心在验证表中查询 T_{ID} 对应的 r、s、b，并验证 $g^r ?= y^{h(w)}r^{r^{-1}} \bmod p$。如果相等，则利用私钥 x，计算 $w=h(s,x)\oplus b$、$t=h(w,r)$、$sk'=h(t,T_{\mathrm{ID}})$，以及 $c'=MAC_{h(w,r)}(w,T_{\mathrm{ID}},sk')$。如果 $c=c'$，则表示认证成功，且双方的会话密钥为 sk'。

虽然身份认证在可穿戴设备、智能终端和卫星移动通信网络中都得到了一定程度的研究，但是目前尚未出现卫星移动通信系统中结合可穿戴设备和智能终端进行持续认证的方案。

3 预备知识

3.1 基于加速度传感器数据的持续认证

Porzi 等[5]提出了一个基于速度传感器和陀螺仪的持续认证方案。该方案在结合可穿戴设备和智能手机的套件下，准确率可以达到 92.1%，并且持续采集 12 h 的数据耗电量仅为 7.2%。本文方案利用该文献的工作成果采集数据，保证合法用户的生物特征能够被攻击者模拟的概率是可忽略的。

方案 2 文献[5]持续认证方案

初始化阶段

设备启动传感器，设置采样率等配置信息。

数据采集阶段

传感器开始采集数据，并对数据进行滤波和降噪等预处理，成为样本数据。

认证阶段

设备取用户的密钥来计算样本数据的消息验证码，连同样本数据传送给认证模块。

认证模块验证消息，并对已存用户信息模板进行匹配，并返回是否通过认证的结果。

3.2 基于口令的卫星移动通信认证方案

Chen 等[14]提出了一种基于认证表的卫星移动通信方案。该方案基于口令，利用加密和签名认证用户身份，保证通信的安全性和高效性。令 $h(\cdot)$ 是一个安全的散列函数，具体过程如图 2 所示。

4 模型与目标

4.1 系统模型

图 1 中各类可穿戴设备及各类智能终端，通过该系统与图右侧的控制中心进行通信。通信的内容包括对用户的身份进行持续认证的信息，以及智能终端采集到的秘密数据。控制中心利用本文提出的结合可穿戴设备与智能终端的持续认证方案，首先对数据发送者的身份有效性进行核实。若通过，则进一步处理收到的秘密数据。否则，忽略该智能终端发来的数据，必要时通知其他智能终端，该终端数据无效。

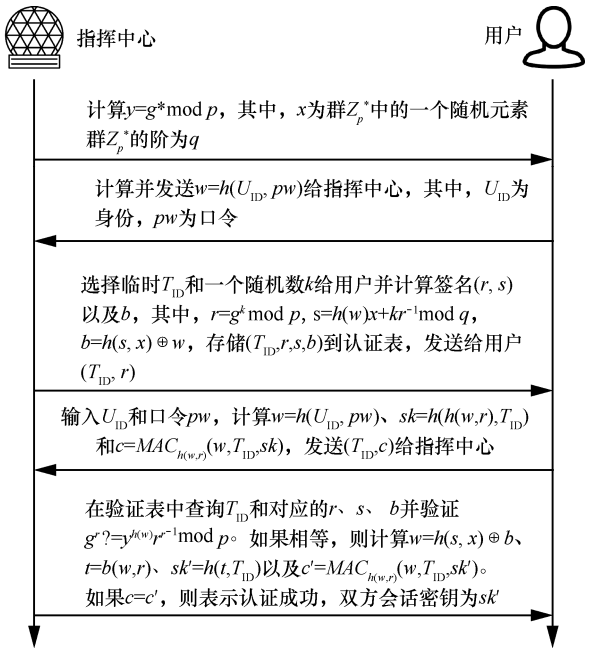


图 2 基于认证表的卫星移动通信方案

4.2 攻击者模型

本文考虑 2 种攻击。第一种攻击来自外部，即非法用户。假定这类攻击者有能力获取用户的可穿戴设备以及智能终端，并且，攻击者可以利用设备和终端发送任意消息给卫星移动通信系统。这类攻击对应可穿戴设备或智能终端因故被攻击者捕获的情况。所以攻击者有能力发送消息。第二种攻击来自内部，即合法用户。假定这类攻击者有能力模仿其他用户发送消息。这类攻击主要用于防止内部的合法用户因故冒充系统内其他合法用户发送假消息的情况。

方案 3 卫星移动通信数据安全传输方案

初始化阶段

指挥中心从阶为 q 的群 Z_p^* 中选择一个随机元素 x 作为私钥，并计算 $y=g^x \bmod p$ 作为公钥。

注册阶段

用户输入身份 U_{ID} 以及口令 pw 并计算 $w=h(U_{\mathrm{ID}},pw)$ 最后发送 w 给指挥中心。

指挥中心选择选择一个临时身份 T_{ID} 和一个随机数 k 给用户，并计算签名 (r,s) 以及 b。其中，

$r = g^k \bmod p$ ， $s = h(w)x + kr^{-1} \bmod q$ ， $b = h(s, x) \oplus w$。最后指挥中心存储 $(T_{\mathrm{ID}}, r, s, b)$ 到认证表中，并发给用户 (T_{ID}, r)。

认证阶段

用户输入身份 U_{ID} 和口令 pw，并计算 $w = h(U_{\mathrm{ID}}, pw)$，$sk = h(h(U_{\mathrm{ID}}, pw), T_{\mathrm{ID}})$，$c = MAC_{h(w,r)}(w, T_{\mathrm{ID}}, sk)$，用户发送 (T_{ID}, c) 给指挥中心。

指挥中心在验证表中查询 T_{ID} 对应的 r, s, b，并验证 $g^r ?= y^{h(w)} r^{r^{-1}} \bmod p$。如果相等，则利用私钥 x，计算 $w = h(s, x) \oplus b$、$t = h(w, r)$、$sk' = h(t, T_{\mathrm{ID}})$ 以及 $c' = MAC_{h(w,r)}(w, T_{\mathrm{ID}}, sk')$。如果 $c = c'$，用户计算 $h(w, r)$。令 *Pseudo* 为一个伪随机函数，计算并发送 $Ps = Pseudo(h(w, r), E \| F)$ 给指挥中心。

4.3　安全目标

本文方案期望达到的安全目标是针对外部攻击者，能够保证环境与用户生物特征数据无法被攻击者得到；针对内部攻击者，能够检测出用户身份异常，并通知控制中心以阻止上述攻击的发生。

5　卫星移动通信系统中结合可穿戴设备与智能终端的持续认证方案

卫星移动通信系统中结合可穿戴设备与智能终端的持续认证方案（CASTWED）首先通过 3.1 节介绍的方法，利用可穿戴设备与智能终端上的传感器，采集周围环境数据 E 以及用户的生物特征 F。采集到的原始数据首先经过可穿戴设备的预处理，将明显不正常或出现极大误差的数据过滤掉。然后，按照通信协议的要求对数据进行压缩和重新编码，组成将要发送的数据分组等待发送。

然后，采用如图 3 所示方法将采集到的 E 和 F 发送给指挥中心。

最终，指挥中心将收到的数据通过 3.1 节中介绍的方法进行分析，并确定用户身份是否有效。

6　安全性分析与性能分析

下面分析上述方案的安全性和性能。

定理 1　如果 *Pseudo* 是一个伪随机函数，*MAC* 是一个安全的消息认证码算法，那么在随机预言机模型下，CASTWED 方案是安全的持续身份识别方案。

证明　针对外部攻击者，如果 E 或 F 能够被攻击者识别，那么攻击者满足条件 1 或条件 2。条件 1：可以得到 $h(w, r)$。条件 2：能够区分 $Pseudo(h(w, r), E \| F)$ 与一个随机函数。条件 2 与 *Pseudo* 为一个伪随机函数矛盾。

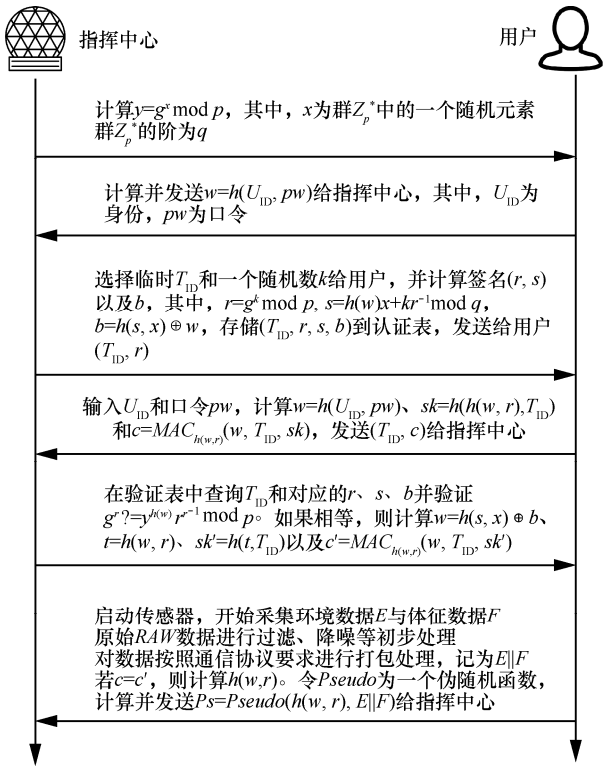


图 3　可穿戴设备与卫星通信的持续认证方案

根据算法 2 的定义，$w = h(U_{\mathrm{ID}}, pw)$。其中，由于在随机预言机模型下，$w$ 可以被视作一个随机数。那么在方案中，由于整个认证阶段只有 $MAC_{h(w,r)}(w, T_{\mathrm{ID}}, sk)$ 和 T_{ID} 被传送给指挥中心。又因为 T_{ID} 与 $h(w, r)$ 独立，所以攻击者必定根据 *MAC* 值获取密钥 $h(w, r)$。如果这样，那攻击者就可以利用获得的密钥伪造任意消息的认证码，这与 *MAC* 是一个安全的消息认证码算法矛盾。

因此，上述 2 个条件都无法满足，攻击者无法获取 E 或 F。

针对内部攻击者，如果攻击者能够通过认证，那么他在无法获取 $h(U_{\mathrm{ID}}, pw)$ 的情况下，只能成功伪造出 E 或 F。这说明该攻击者能够模拟其他用户。根据 3.1 节的介绍，这样的概率可以忽略不计。

综上，CASTWED 是一个安全的持续身份识别方案。

证毕。

最后，本文分析 CASTWED 方案的性能。在卫星移动通信系统中，本文方案假定在 Ku 波段 60 Mbit/s 传输速率下工作。

在模拟实验中，考虑到系统需要支持 10 万用户的并发访问，所以将 ID 长度设置为 17 bit（2^{17}=131 072）。在 Intel i3 处理器和 4 GB 存储器下模拟卫星在处理 10 万用户的数据时处理延迟约为 0.9 s。本文选择 AES-128 算法作为伪随机函数，SHA-1 为散列函数，HMAC 作为 MAC 方案。则相应的 r 、s 和 b（方案 3 中签名 (r,s) 以及 b ）分别为 512 bit、512 bit 和 160 bit。于是在加入用户 ID 之后，每个用户与卫星系统之间每次传递的数据分组大小为 1 201 bit，相应地，在 60 Mbit/s 下 10 万用户并发访问时候的发送延迟约为 20.02 s。采用 AGI Satellite Tool Kit（STK）进行模拟卫星组网，组网方案如图 4 所示，共包括 33 颗中轨道卫星，卫星高度为 8 042 km，这也使网络的传播时延可以忽略不计。此时，并发用户数目与卫星移动通信传输速率的关系如图 5 所示。可以看到，CASTWED 方案在 60 Mbit/s 传输速度的限制条件下，可以支持 110 294 位用户并发进行持续认证。

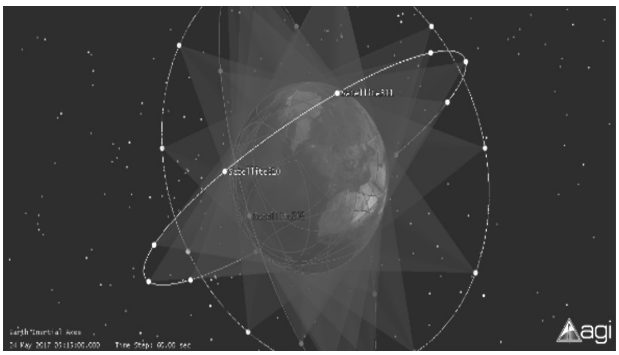


图 4 使用 STK 进行模拟卫星组网

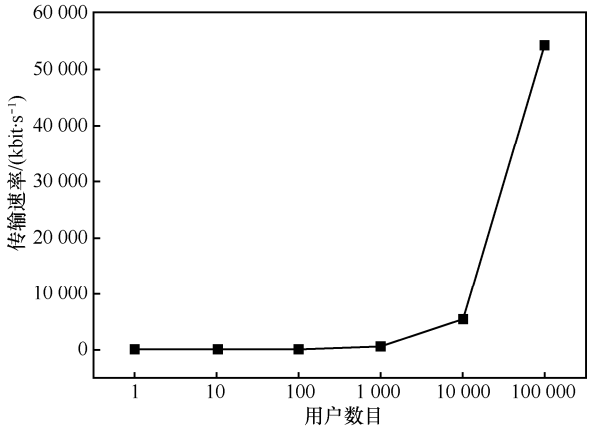


图 5 并发持续认证用户数目与卫星移动通信传输速率关系

7 结束语

本文针对卫星移动通信系统 Ku 波段 60 Mbit/s 传输速率下，用户持续身份认证问题展开研究。通过将可穿戴设备与智能终端相结合的方式，设计并实现了一个安全高效的持续认证方案。本文提出的方案能够支持 10 万人并发持续认证。

未来工作包括 3 个方向。1) 继续深入研究所用的传感器，并扩展研究更多类型的传感器，以期能够补充更多的持续认证方法。2) 学习深度学习等理论与算法，以期能够找到细粒度且准确的持续认证算法。3) 研究其他轻量级卫星移动通信安全传输方案，在保证安全性的同时提高数据传输效率。

参考文献：

[1] CHU C T, CHIANG H K, HUNG J J. Dynamic heart rate monitors algorithm for reflection green light wearable device[C]//2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS). 2015: 438-445.

[2] SON D, LEE J, QIAO S, et al. Multifunctional wearable devices for diagnosis and therapy of movement disorders[J]. Nature Nanotechnology, 2014, 9(5): 397-404.

[3] ZHENG Y L, YAN B P, ZHANG Y T, et al. An armband wearable device for overnight and cuff-less blood pressure measurement[J]. IEEE Transactions on Biomedical Engineering, 2014, 61(7): 2179-2186.

[4] SARKAR S, JOHNSTON T P, BRAN C, et al. Wearable user device for use in a user authentication system[P]. US20160253487. 2016.

[5] PORZI L, MESSELODI S, MODENA C M, et al. A smart watch-based gesture recognition system for assisting people with visual impairments[C]//The 3rd ACM International Workshop on Interactive Multimedia on Mobile & Portable Devices. ACM, 2013: 19-24.

[6] GAFUROV D, SNEKKENES E, BOURS P. Gait authentication and identification using wearable accelerometer sensor[C]//2007 IEEE Workshop on Automatic Identification Advanced Technologies. 2007:220-225.

[7] TIJERINA K K, DORIS-DOWN A, WILCZYNSKI M A, et al. Wearable device authentication[P]. US20160191511. 2016-6-30.

[8] WONG A, STARNER T E, WEAVER J. Wearable computing device authentication using bone conduction: U.S. Patent 9,277,334[P]. 2016-3-1.

[9] 段利艳, 刘晖. 智能可穿戴设备的无线技术认证[J]. 安全与电磁兼容, 2016(3): 43-44.
DUAN L Y, LIU H. Wireless technology certification of intelligent wearable device[J]. Safety and EMC, 2016(3): 43-44.

[10] 裘玥. 智能可穿戴设备信息安全分析[J]. 信息网络安全, 2016(9): 79-83.
QIU Y. Security analysis of the information of wearable devices[J]. Net Info Security, 2016(9): 79-83.

[11] 落红卫, 魏亮, 徐迎阳. 可穿戴设备安全威胁与防护措施[J]. 电信网技术, 2013(11): 9-11.
LUO H W, WEI L, XU Y Y. Security threats and protection methods for wearable devices[J]. Telecommunications Network Technology, 2013(11): 9-11.

[12] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.

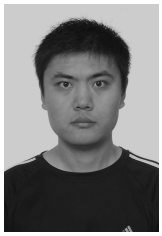
[13] GUSTAFSON B. Satellite based key agreement for authentication[P]. US20150365824. 2015-12-17.

[14] CHEN C L, CHENG K W, CHEN Y L, et al. An improvement on the self-verification authentication mechanism for a mobile satellite communication system[J]. Applied Mathematics & Information Sciences, 2014, 8(1L):97-106.

[15] LIN H Y. Efficient dynamic authentication for mobile satellite communication systems without verification table[J]. International Journal of Satellite Communications and Networking, 2016, 34(1): 3-10.

[16] ELMASRI M H, MEGAHED M H, ELAZEEM M H A. Design and software implementation of new high performance group key management algorithm for tactical satellite[C]//33rd National Radio Science Conference (NRSC). 2016: 149-158.

作者简介：



徐日新（1985-），男，山东日照人，北京理工大学博士生，主要研究方向为身份认证协议设计与安全性分析、侧信道攻击。

陈小兵（1976-），男，四川广安人，北京理工大学博士生、高级工程师，主要研究方向为信息安全、Web 渗透、数据库安全。

祝烈煌（1976-），男，浙江衢州人，博士，北京理工大学教授，博士生导师，主要研究方向为密码算法及安全协议、天地一体化网络安全、物联网安全、云计算安全、大数据隐私保护、移动互联网安全、可信计算。