



基于手机令牌的移动应用双向身份认证方案研究^{*}

郑兆华, 彭金莲, 程杰仁

(海南大学信息科学技术学院 海口 570228)

摘要:随着移动信息化的发展,移动应用的安全问题已成为用户关注的焦点。身份认证存在多种解决方案,其中动态口令技术是目前身份认证问题的最有效解决方案。在分析目前动态口令存在缺陷的基础上,提出了一种改进的基于手机令牌的挑战/应答动态口令身份认证方案,它以指纹作为令牌使用凭证,能双向可信认证,并以分段双通道方式进行加密通信。此外,对新方案进行了安全性分析。分析结果表明该方案具有安全性高、使用简便、成本低的特点,完全满足移动应用通信中安全级别较高的身份认证要求。

关键词:动态口令;手机令牌;身份认证;安全;移动信息化;挑战/应答

doi: 10.3969/j.issn.1000-0801.2014.09.012

Research on Application Bidirectional Identity Authentication Scheme Based on Mobile Phone Token

Zheng Zhaohua, Peng Jinlian, Cheng Jieren

(College of Information Science and Technology, Hainan University, Haikou 570228, China)

Abstract: With the development of mobile information, security problems of mobile applications had become the focus of attention of the user. Authentication has many solutions. The dynamic password authentication technology is currently the most effective solution. After analyzing the current dynamic password shortcomings, a dynamic password authentication scheme based on improved mobile phone token to challenge / response was proposed. It uses fingerprint as the evidence of token, and can be two-way authentication, and has segment of double channel encryption communication. In addition, the security was analyzed. Analysis results show that the scheme is convenient to use and has high security and low cost. The scheme fully meets the higher security level of identity authentication on application requirements in mobile communication.

Key words: dynamic password, mobile phone token, identity authentication, security, mobile informatization, challenge/response

1 引言

随着移动互联网的迅速发展,越来越多企业希望通过移动信息化提高效率。作为移动信息化核心的移动应用已成为企业典型应用。移动应用将企业核心业务数据延伸到移动终端中运用,然而安全问题是制约企业移动信息化发

展的一个主要瓶颈。移动应用是在开放移动互联网场景下的频繁交互,需要认证用户的合法性。目前绝大部分移动应用采用静态口令认证,其安全性难以控制,容易被猜测、窃听和暴力破解,不能满足企业移动信息化的安全要求。动态口令认证技术能够弥补静态口令的不足,能满足移动应用的安全认证要求。

^{*} 国家自然科学基金资助项目(No.61363071),海南大学青年基金资助项目(No.qnjj1255),海南大学应用科技学院项目(No.yykj-ky-2009-9)



2 动态口令技术

2.1 动态口令实现原理及实现机制

动态口令,又叫一次性口令,是指在认证中加入了时间、随机数等不确定因素,使用专门算法生成的一个不可预测的随机数字。每个密码只能使用一次,使得攻击者无法通过窃取口令或重放攻击来获取登录权限。动态口令被公认为是最安全的身份认证方式之一,并获得广泛应用。根据动态因素不同,可分为时间同步机制、事件同步机制和挑战/应答机制^[1],具体介绍如下。

- 时间同步机制以登录时间作为动态因素。优点是实现简单,但对时间准确度要求较高,技术上难以实现。数据在网络上传输和处理存在一定时延,增大了重放攻击和暴力破解的可能性^[2]。
- 事件同步机制是以事件的次序作为动态因素。该机制比较容易实现,不需要特殊硬件的支持,但同样存在失去同步的风险。
- 挑战/应答机制是以认证服务器发出的挑战码作为动态因素。它有很高的安全性,并不涉及同步问题,是目前最可靠的认证方法之一,但缺点是存在单向认证和需人工输入挑战码。

时间同步和事件同步机制容易失去同步,可靠性不是很高;挑战/应答机制虽然增加用户输入步骤,但是可靠性最好。如果能自动输入挑战码并双向认证,就是一种较优的解决方案。

2.2 动态口令的实现方式

实现方式分为硬件令牌和软件令牌。目前大部分采用硬件令牌,如中国银行 e-token、网易将军令、盛大密宝、QQ 令牌等。硬件令牌是一种采用内置电源、存储器、密码计算芯片和显示屏的设备,具有使用便利、安全性高等特点^[3]。但它“认牌不认人”,虽然携带方便,但也容易丢失;缺少通信模块,认证服务器无法对其管理和更新数据,一旦失去同步,将无法使用;实施成本较高,这对于预算有限的中小企业来说,显然是不现实的。

软件令牌指使用软件实现的令牌。随着移动时代的到来,智能手机的迅速普及为软件令牌带来了发展机遇。软件令牌无需用户携带额外的设备,相对硬件令牌来说,手机有通信模块,功能更强大,能有效解决上述硬件令牌的缺点。软件令牌必将成为行业的发展趋势。

软件令牌具有安全性高、使用便捷、实施成本低的特点,

非常适合中小企业使用。韦广剑提出基于 Android 令牌的身份认证系统^[4]是基于时间同步机制的,存在时间失步和被跟踪破解的风险;郭建昌等提出一种电信级手机令牌动态口令系统^[5],但对于普通企业来说,并不具备实施条件;叶晰也提出手机令牌方案^[6],但是其使用过时的 J2ME 技术。本文提出一种基于手机令牌的身份认证新方案。该方案采用更安全的指纹而不是 PIN 码作为使用凭证,能真实地绑定使用者和手机令牌的关系;能够实现双向可信认证,并以分段双通道(互联网+短信)方式进行加密通信;能远程初始化手机令牌,方便令牌发放。

3 身份认证方案

身份认证方案包括手机令牌注册和身份认证两部分。手机令牌注册包括手机令牌初始化和令牌发放过程。身份认证是指手机令牌生成动态口令,然后通过身份认证系统进行身份认证。涉及的符号及其说明见表 1。

表 1 符号和说明

符号	说明
U	用户
MT	手机令牌
AS	认证服务器。拥有加密算法 ECC 私钥
R	不重复随机数
TPK	临时通信用的 AES 密钥
HFC	硬件特征码
FFC	指纹特征码
RK	根密钥,是 MT 和 AS 共有 AES 密钥
$F_n(R)$	对随机函数进行特殊散列处理,算法保密
GC(S)	将长度为 20 的字符串 S 进行分组,高低位组合和异或运算后,生成 8 位动态口令
SHA1(S)	对字符串 S 进行 SHA1 摘要处理
SGPB(S)	先对 S 进行 SHA1 摘要处理,然后用 AS 的 ECC 公钥对摘要数字签名
SGPR(S)	先对 S 进行 SHA1 摘要处理,然后用 AS 的 ECC 私钥对摘要数字签名

3.1 手机令牌注册过程

注册过程是指手机令牌(MT)向认证服务器(AS)登记指纹信息、设备信息和账户相关信息,并初始化的过程,如图 1 所示。具体说明如下。

(1)用户(U)扫描指纹,登记注册信息。指纹具有普遍性、唯一性和永久性等特征,是世界公认的身份识别标识,是一种最高水平的安全保密解决方案^[7]。指纹加密存储在手机令牌内,并作为使用者的凭证,只有和登记指纹相吻

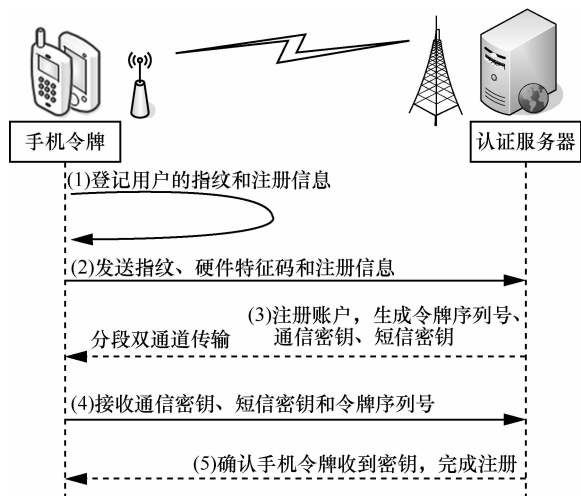


图1 注册过程

合,才能使用该令牌。注册信息主要包括账户、姓名、性别、E-mail、手机号等注册信息。其中手机号必填,作为除互联网之外的信道,用于传输敏感信息。

(2)发送指纹、硬件特征码和注册信息到认证服务器。硬件特征码 $HFC=SHA1(\text{手机IMEI}+\text{SIM卡IMSI})$,用于标识硬件运行环境。具体处理步骤如下。

生成随机数 $R1$ 和临时通信密钥 TPK ; 明文 $(PT)=\text{指纹}+\text{注册信息}+HFC+R1$,进行数字签名 $SGPB(PT)$;用 AS 的私钥加密 TPK ;用 TPK 加密明文。

处理后,将密文、加密的 TPK 和签名一起发送给 AS 。

(3)注册账户,生成令牌序列号、通信密钥和短信密钥。 AS 用私钥解密签名和 TPK ,然后用 TPK 解密密文。 $SHA1(\text{明文})$ 与解密后的签名进行比较,以验证信息完整性。验证通过后,注册用户,提取指纹特征码(FFC)。把当前时间、 FFC 、 HFC 和注册信息使用专门算法处理后,生成令牌序列号(SN)、通信密钥(CK)和短信密钥(SK)。将 CK 、 SK 、 HFC 和 FFC 用 AS 的公钥加密存储在数据库。密钥 CK 和 SK 属于核心机密,使用短信和互联网双通道传送给 MT 。具体处理过程如下。

- 生成随机数 $R2$,对明文随机数 $R1$ 进行 $F_n(R1)$ 处理。
- 将 SK 分为 $SK1$ 和 $SK2$,将 CK 分为 $CK1$ 和 $CK2$ 。
- 互联网通道回应:首先, $(PT)=SN+CK1+SK2+F_n(R1)+R2$,进行数字签名(DS)= $SGPR(PT)$;然后,用 TPK 加密明文;最后,将密文和数字签名通过互联网通道回应给手机令牌。
- 短信通道回应类似互联网回应,明文是 $(CK2,SK1,F_n(R1),R2)$,最后短信给令牌注册手机号。

由于密钥分段和双通道传输,只要黑客不能在全部通道

截获所有信息,就不能复原密文。在不能复原密文的情况下,即使窃取了密钥,也无法破解密文,从而保证了密钥安全。

(4)接收通信密钥、短信密钥和令牌序列号,令牌初始化完成。具体处理过程如下。

- 对于互联网通道的处理:首先, MT 使用 AS 公钥对签名解密,用缓存的密钥 TPK 进行解密密文;然后, $SHA1(\text{明文})$ 与解密的签名比较,以验证数据完整性,对缓存随机数 $R1$ 进行 $F_n(R1)$ 处理,与明文 $F_n(R1)$ 比较,以对认证服务器进行可信认证。如果这两个比较均通过,表明 MT 收到的数据完整,认证服务可信;最后,对明文进行处理得到 SN 、 $CK1$ 、 $SK2$ 。
- 短信通道处理类似互联网通道,最终处理得到 $CK2$ 和 $SK1$ 。
- $CK=CK1+CK2,SK=SK1+SK2$ 。将 SN 设置到手机令牌。使用根密钥(RK)加密 CK ,用 CK 加密 SK ,并存储到手机令牌。
- 发送确认通知。生成随机数 $R3$,对 $R2$ 进行 $F_n(R2)$ 处理,对明文数字签名 $SGPB(F_n(R2)+R3)$ 。使用通信 CK 加密明文,用公钥加密 SN 。最后将密文和签名加密 SN 回应 AS 。
- AS 收到后,用私钥解密 SN ,从数据库检索对应通信密钥 CK 解密密文。 $SHA1(\text{明文})$ 和其私钥解密的签名比较。将缓存的 $R2$ 进行 $F_n(R2)$ 处理,然后和明文 $F_n(R2)$ 比较。比较均通过后,表明数据完整, MT 可信并正确收到密钥了。

整个过程中,签名用于确保传输数据的完整性。 F_n 是算法保密的函数,用于 MT 与 AS 进行双向可信认证。 AS 能用 ECC 私钥解密,表明其可信。通过密钥分段双通道传输数据以及多级加密存储等方式,多方面提高密钥安全性,保障了令牌的安全性。

3.2 认证过程

用户扫描指纹,启用手机令牌并产生动态口令,然后发送给认证服务器进行身份认证,如图2所示。具体说明如下。

(1)扫描指纹,启用手机令牌,发送 SN 。用户在手机令牌上扫描指纹验证身份,然后将 SN 发送给认证服务器。具体处理过程如下。

生成随机数 $R1$;明文 $(PT)=F_n(SN)+R1$,进行数字签名 $SGPB(PT)$;用 AS 公钥对 SN 加密;用 CK 加密明文,并与加密的 SN 和签名一起发送给 AS 。

(2)生成挑战码和口令算法密钥 K 。 AS 用私钥解密 SN ,

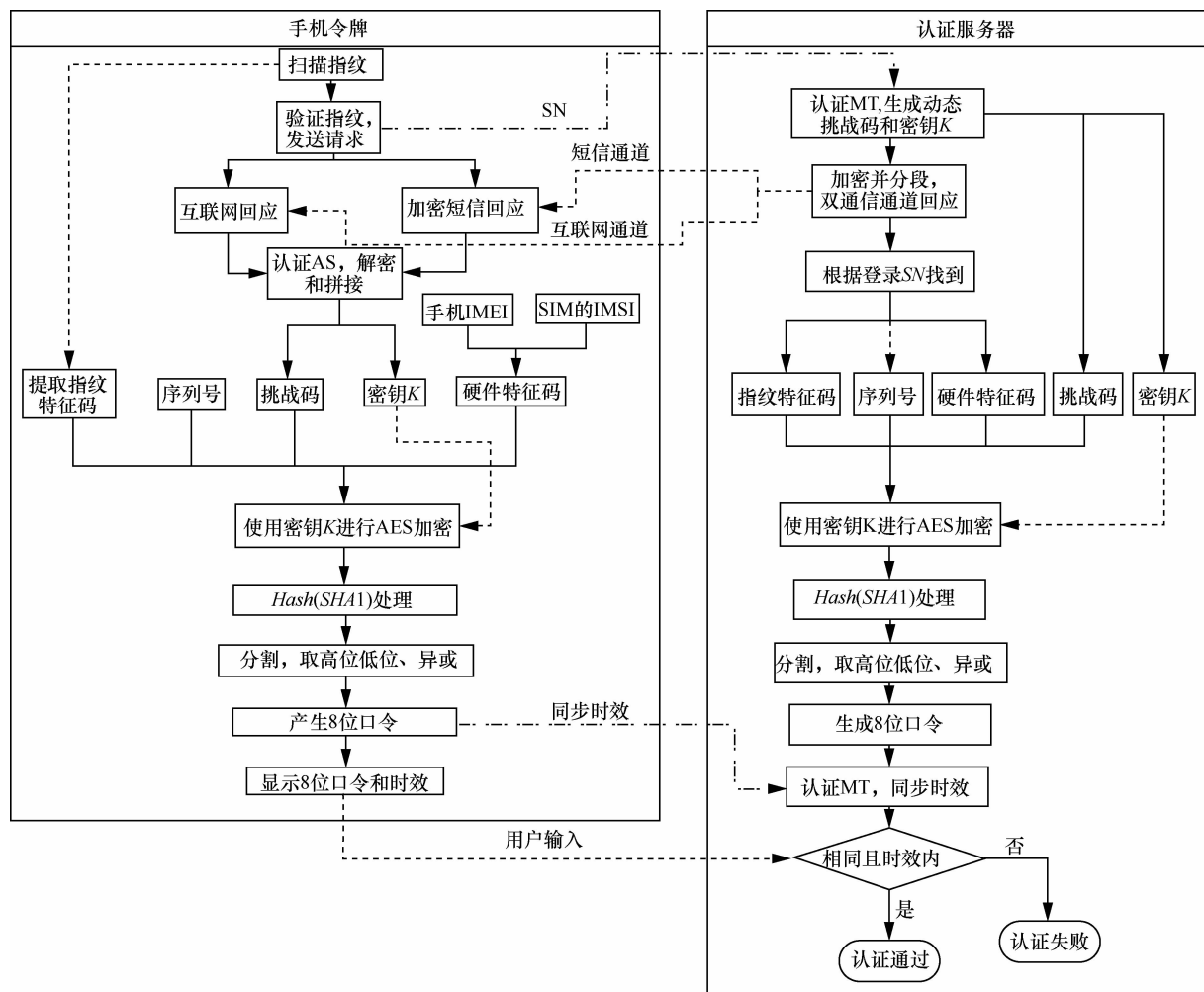


图2 认证过程

并根据 SN 查找对应的密钥 CK 来解密密文。通过 $SHA1$ (明文) 和解密后的签名比较, 确认数据完整性。将 SN 进行 $F_n(SN)$ 处理, 然后通过和明文中的 $F_n(SN)$ 比较, 对令牌可信认证。比较均通过后, AS 使用 SN 、特征码和当前时间作为影响因素, 生成随机的不重复挑战码 C 和口令算法密钥 K 。由于 C 和 K 属于机密信息, 关系着动态口令安全性, 需要对其进行分段和双信道传输, 具体步骤如下。

算法密钥 K 分为 $K1$ 和 $K2$ 两部分, 挑战码 C 分为 $C1$ 和 $C2$ 两部分; 产生随机数 $R2$; 互联网通道回应: 首先, 明文 $(PT)=K1+C2+F_n(R1)+R2$, 进行数字签名 $SGPR(PT)$; 然后, 用 CK 加密明文; 最后, 将密文和签名通过互联网通道回应手机令牌请求; 短信通道回应类似互联网处理, 明文是 $K2+C1+F_n(R1)+R2$, 最后短信给令牌注册手机。

将信息分段和打乱次序, 提高破解难度, 增加安全性。 $F_n(R1)$ 用于可信认证。为了节约成本, $C1$ 和 $K2$ 相对短小,

保证一条短信就可发送。

(3) 手机令牌生成动态口令, 具体过程如下。

- 互联网信道处理: MT 用密钥 CK 解密密文。通过 $SHA1$ (明文) 与解密签名比较来判断数据完整性。对缓存的 $R1$ 进行 $F_n(R1)$ 处理, 然后通过和明文中的 $F_n(R1)$ 比较, 从而认证服务器可信。最后得到 $C2$ 和 $K1$ 。
- 短信信道处理类似互联网信道, 最后获得 $C1$ 和 $K2$ 。
- 挑战码 $C=C1+C2$, 口令算法密钥 $K=K1+K2$ 。
- 提取指纹特征码 (FFC)。 $S=FFC+HFC+SN+C$ 。用密钥 K 对 S 进行 AES 加密, 然后 $SHA1$ 摘要, 得到长度 20 的字符串 ABS 。通过 $GC(ABS)$ 处理得到 8 位的动态口令, 并向 AS 发送时效同步通知, 时效为 60 s。

(4) 认证服务器按同样算法生成动态口令。

(5) 同步时效。 AS 收到令牌的通知后开始同步计算口令的时效。

(6)验证动态口令。用户输入 MT 的动态口令和账户,以加密形式发送到 AS 进行身份认证。AS 解密收到信息,并验证账户、动态口令及时效,认证过程结束。

4 安全性分析

- 关于本文提出方案的安全性分析如下。
- 截获/重放攻击。即使攻击者窃听到用户的动态口令,但是由于动态口令是一次性的,发送给 AS 也不能通过认证。通信中引入不重复随机数 R ,当入侵者进行重放攻击时,因为重复随机数,而拒绝请求,重放攻击失败。
 - 小数攻击。手机令牌和认证服务器的通信过程是采用 AES 加密和 ECC 签名,安全性很高,攻击者无法窃取敏感信息,也无法进行小数攻击。动态口令以动静因子相结合的算法产生,并无规律可循,也避免了小数攻击。
 - 中间人攻击。手机令牌和认证服务器采用加密通信和双向可信认证,口令和密钥等敏感信息通过分段双通道加密发送。中间人攻击将因为这些措施而攻击失败。
 - 暴力破解。该系统的安全性依赖于 AES 加密算法和 ECC 加密算法的安全性。AES 是公认最安全的对称加密算法^[8],是目前公认最高比特加密强度的公钥算法^[9],目前没有有效可行的破解办法。AES 和 ECC 确保攻击者无法获取有效信息,也无从攻击。认证服务器的账户锁定功能使得蛮力攻击和猜测攻击难以成功,因为在有限次数内猜中动态口令的概率极小。
 - 保证物理安全。即使用户的移动终端丢失或者被盗,由于令牌使用指纹凭证,只能用户本人使用。指

纹也是口令计算因素之一,缺少了指纹,将无法生成动态口令。

5 仿真结果及分析

实验环境包含运行在 Android 系统上的手机令牌仿真程序和利用 Java 开发的仿真认证服务器两部分。其中手机令牌运行在三星的 Note II 智能手机上,认证服务器运行在部署了 Tomcat 6.0 的 PC 上,设备的主要参数见表 2。

表 2 设备主要参数

实验设备	OS	CPU	RAM
Note II	Android 4.1	1.6 GB 4 核	2 GB
PC	Windows7 x64	2.5 GB 4 核	4 GB

首先,进行算法功能性测试。经过多次测试,结果表明算法正确,功能正常。然后,测试口令生成效率。图 3 是测试 50 次的实验结果。

从图 3 可以看出生成口令过程中,手机令牌耗时为 8~20 ms,平均 10.8 ms;认证服务器耗时为 1~4 ms,平均 2.3 ms。因此,该认证方案具有非常高的运行效率。

6 结束语

随着互联网和智能手机产业的发展,手机令牌动态口令技术具备覆盖范围广、安全性高、成本低和携带方便等特点,是未来移动应用身份认证解决方案的发展方向。本文提出一种手机令牌身份认证方案,它使用指纹作为令牌使用凭证,精确地绑定手机令牌和使用者的关系,采用分段双通道方式传送密钥和挑战码,并在通信过程中能够双向可信认证;口令生成算法将动静因子结合,并以 AES、SHA1 算法为基础;该方案运用手机作为令牌载体,实现一种软件令

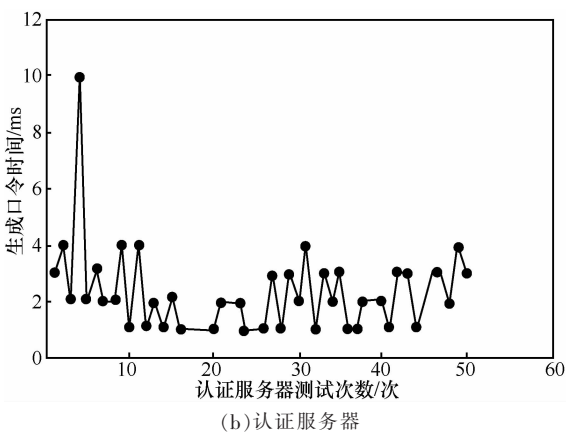
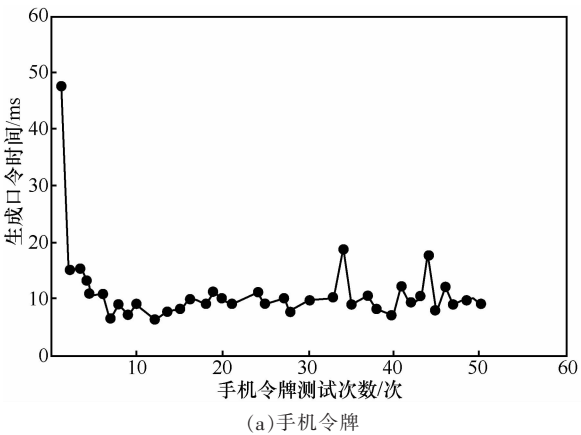


图 3 生成口令性能

- 7 马守明, 王汝传, 叶宁. 基于信誉度集对分析的 WSN 完全数据融合. 计算机研究与发展, 2011, 48(8): 1652~1658
- 8 李小亚, 潘家辉. 无线传感器网络能量平衡的数据汇聚路由算法. 华南师范大学学报(自然科学版), 2012, 44(2): 53~57
- 9 Luo C, Wu F, Sun J, *et al.* Compressive data gathering for large-scale wireless sensor networks. Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, Beijing, China, 2009: 145~156
- 10 Luo J, Xiang L, Rosenberg C. Does compressed sensing improve the throughput of wireless sensor networks. Proceedings of 2010 IEEE International Conference on Communications (ICC), Cape Town, South Africa, 2010: 1~6
- 11 Xiang L, Luo J, Vasilakos A. Compressed data aggregation for energy efficient wireless sensor networks. Proceedings of 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Salt Lake City, Utah, USA, 2011: 46~54
- 12 Gilbert A C, Strauss M J, Tropp J A, *et al.* One sketch for all: fast algorithms for compressed sensing. Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing, San Diego, California, USA, 2007: 237~246
- 13 Park J, Jung B C, Kim J M, *et al.* Sparse signal recovery with parallel orthogonal matching pursuit and its performances. Journal of the Korea Institute of Information and Communication Engineering, 2013, 17(8): 1784~1789
- 14 Zhang W, Huang B, Zhou T. An improvement on StOMP for

sparse solution of linear underdetermined problems. Proceedings of 32nd Chinese Control Conference (CCC), Xi'an, China, IEEE, 2013: 1951~1956

- 15 Jeong Y S, Han Y H, Park J J, *et al.* MSNS: mobile sensor network simulator for area coverage and obstacle avoidance based on GML. EURASIP Journal on Wireless Communications and Networking, 2012(1): 1~15

[作者简介]



赵建军,男,保定学院实验师,主要研究方向为数据挖掘、网络安全。

王怀宇,男,保定学院讲师,主要研究方向为数据挖掘、嵌入式系统。

赵泽阳,男,保定学院硕士生,主要研究方向为数据收集。

陈生昌,男,博士,浙江大学教授、博士生导师,主要研究方向为压缩感知理论、数据收集技术、计算地球物理。

(收稿日期:2014-03-20)

(上接第91页)

牌,具有使用便捷、安全性高、运行效率高、成本低、功能强大和人性化等特点,非常适合移动应用的身份认证。

参考文献

- 1 郑强, 高能, 张令臣. 基于 SM3 算法的动态口令卡的设计与实现. 计算机应用与软件, 2013, 30(2): 14~17
- 2 张利华, 章丽萍, 张有光等. 基于口令的远程身份认证及密钥协商协议. 计算机应用, 2009, 29(4): 924~927
- 3 林元明. 基于手机令牌的身份认证系统的研究与实现. 厦门大学硕士学位论文, 2009
- 4 韦广剑. 基于 Android 令牌的动态密码认证系统的研究与实现. 武汉理工大学硕士学位论文, 2012
- 5 郭建昌, 郭茂文, 黎艳. 一种电信级手机令牌动态口令系统的架构设计及其实现. 电信科学, 2012, 28(10): 94~98
- 6 叶晰, 叶依如, 岑琴. 基于手机令牌的动态口令身份认证系统的实现. 计算机系统应用, 2010, 19(10): 32~36
- 7 刘超凡, 张永良, 肖刚等. 基于滚动指纹数字签名的电子商务安全认证. 计算机应用, 2012, 32(2): 475~479
- 8 赵新杰, 王韬, 郭世泽等. AES 访问驱动 Cache 计时攻击. 软

件学报, 2011, 22(3): 572~591

- 9 闫茂德, 纪志强, 贺显曜等. AES 与 ECC 混合加密算法的无线数据通信系统设计. 微电子学与计算机, 2007, 24(7): 135~138

[作者简介]



郑兆华,女,海南大学信息科学技术学院讲师,主要研究方向为信息安全与移动互联网应用。

彭金莲,女,海南大学信息科学技术学院教授,主要研究方向为农业信息技术与网络安全。

程杰仁,男,海南大学信息科学技术学院教授,主要研究方向为网络安全。

(收稿日期:2014-08-20)