基于加密编码矢量的农业无线传感网数据安全存储方法

张 巍[1,2] 史兴燕[2] 崔茂齐[3]
(河南省农业高新科技示范园 郑州 451450)[1] (河南农业职业学院 郑州 451450)[2]
(沧州师范学院 沧州 061001)[3]

摘 要 无线传感网为精准农业生产环境监测提供了一种有效的解决方案。针对当前农业生产中无线传感网感知数据传输和存储过程中存在的安全性不高、存储效率不佳的问题,在研究农业无线传感网主要特征的基础上,分析了云存储技术对农业传感器感知数据存储的有效性,利用改进的网络编码技术降低了传感器感知数据在传输汇聚时对无线网有限带宽的占用率,给出了基于加密编码矢量方法的农业无线传感网感知数据传输、存取安全性和效率分析,提出了一种基于加密编码矢量的农业无线传感网感知数据信息的安全存储新方法。大田生产环境测试结果表明,基于网络编码的加密编码矢量方法安全性较高,在数据量显著增加的情况下传输性能可进一步得到提升,从而验证了本方法的合理性和实用性。

关键词 精准农业,无线传感网,云存储,加密编码矢量
中图法分类号 TN301.4 **文献标识码** A

Method for Data Storing Based on Coding Vector Encryption in WSNs

ZHANG Wei[1,2] SHI Xing-yan[2] CUI Mao-qi[3]
(Henan New and High Technology Agriculture Park, Zhengzhou 451450, China)[1]
(Henan Vocational College of Agriculture, Zhengzhou 451450, China)[2] (Cangzhou Normal University, Cangzhou 061001, China)[3]

Abstract With the development of wireless sensor networks (WSNs), an effective solution was provided by WSNs in precision agriculture production environmental monitor fields. Considering the WSNs shortages in agricultural production, especially in data transmission security and storage efficiency, this paper firstly summaried the main features of the agricultural WSNs and analyzed the good results to introduce cloud computing storage techniques. Then, the lower convergence of sensing data transmission process was approved by the scientific analysis to show importance for limited bandwidth with optimizaed network coding technique. Finally, with the help of coding vector encryption in WSNs, a new method for secure storage of sensor data information of agricaltural WSNs based on coding vector encryption was proposed. All the field testing results show that the method is rational and practical, and it can achieve a high encryption security based on network coding and a significant enhancement in the data transmission process.

Keywords Precision agriculture, Wireless sensor networks, Cloud storage, Coding vector encryption

高效集成了遥感技术(RS)、地理信息系统(GIS)和全球定位系统(GPS)的精准农业(precision agriculture)已成为引领我国农业发展的重要方向。精准农业有机结合了传统农业农艺、农机装备和先进的 3S 高新技术,通过对农业生产过程中的时间、空间差异数据的采集和处理,实现田间时空变量信息数据的测量和感知,依据农作物生长所处的局部土壤肥力、杂草、病虫害等信息预测作物产量在时空上的差异变化,实现变量化田间生产管理、施肥、灌溉和用药,精确优化农业的投入,获得最高的产量和效益[1,2]。

各类先进传感器设备及其稳定可信的工作状态是精准农业实现的重要前提[3]。农业生产中,种植的作物生长情况极易受到空气温度、湿度、风速、光照等自然环境因素和土壤含水率、pH 值、坚实度、氮磷钾肥力等局部因素的影响,往往会产生一定的长势差异,这就需要各类传感器及其网关节点能够尽可能准确、实时地上报监测到的数据信息[4,5]。无线传感网(Wireless Sensor Networks, WSN)为精准农业的实现提供了高效解决方案,并在农业生产中得到了飞速发展和广泛应用。然而,因 WSN 在通信、计算、存储和功耗等方面存在一定的不足,传统的数据处理模式和管理方法难以满足精准农业无线传感网对信息源的处理要求,在一定程度上限制了 WSN 在农业生产领域的深入应用[6-8]。

为解决上述问题,本文提出一种新的精准农业无线传感网数据加密编码矢量云存储方法:采用 ZigBee 技术构建精准农业无线通信网络,通过布控于农田现场的网关节点搜集农业生产实测数据;基于网络数据加密编码矢量方法和分布式数据存储模式,在保障数据可靠性和安全性的前提下,降低对

本文受国家自然科学基金项目(51302221)资助。

张 巍(1969—),男,硕士,副教授,主要研究方向为信息处理,E-mail:hnnxzw@126.com(通信作者);史兴燕(1980—),女,硕士,讲师,主要研究方向为图形图像处理;崔茂齐(1968—),男,硕士,讲师,主要研究方向为自动控制技术。

带宽、网关节点计算能力和存储资源等的占用率，实现精准农业大规模测量数据信息的管理和维护。

1 基于云存储的无线传感网

传统的无线传感网的结构类型可以划分为3种：①单层结构；②基于簇的单层结构；③多层结构。①型结构中，各类传感器功用相同，可实现数据采集、数据处理和发送汇聚等基本功能；②型结构中，同型传感器先构成一个簇，并将同型传感器的感知数据汇聚到簇头并由其转发簇成员的数据；③型结构中，依传感器类型的不同而分别组成不同的层级，每层可设置一个中心节点，并由最高层级的中心节点与汇聚节点相连接。由于无线传感网中数据处理密度和转发量较大，加之单个传感器的能量有限，往往造成中心节点或者汇聚节点发生数据丢失和能量过早耗尽而死亡等问题[9,10]。

1.1 体系结构

图1中给出了一种基于云存储的无线传感网体系结构，主要由云节点、域和主控节点构成。图中SP(Sink Point)表示汇聚节点。

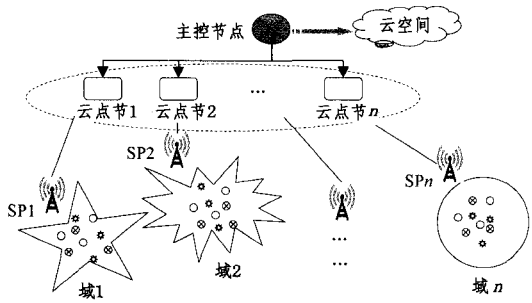

图1 基于云存储的无线传感网体系结构

定义1 在云存储无线传感网中，可与周围传感器通信并收集各传感器数据信息的特殊传感器节点称为云节点。

定义2 在云存储无线传感网中，同一云节点内的各个传感器所构成的集合称为域。

云节点不仅可以完成普通传感器的数据采集功能，而且具有比普通传感器更为丰富的计算资源，是一种特殊的汇聚节点。云节点可以将域中的数据信息存储于云空间中，从而使整个无线传感网形成一个虚拟汇聚节点网。

各个域中传感器的组织形式所依据的规则为：①以汇聚节点 SP 为中心，同类型传感器自组为一个无线传感网子网，数据统一发送到该 SP 处；②同类传感器在无法通信时，由非同类传感器充当临时网关；③云中部署无线传感网处理软件，可借助云来对传感器进行调度和优化。通过配置IEEE 802.11协议栈来构建Ad hoc网络所形成的无线传感网具有子网规模小、数据传输效率高和全局控制效果好等优点[11]。

1.2 采集数据的分布式安全存储

借助云存储环境，可有效利用云平台的存储低价、后台维护便捷等优势，提升无线传感网信息的实时远程容灾存储和备份。复制是一种提高冗余可靠性的直接方法，擦除码作为复制的改进可提供更为高效的存储效率，并可降低对网络传输资源的占用率[12]。

擦除码的工作原理[13]是：①将数据文件 M 分为 k 个等份(不足等份通过末尾补0的方式补足)，每份的片段大小为 M/k；②基于最大距离分割码算法，将这些片段编码成 n 个片段，分别存储于 n 个存储节点上；③解码 k 个片段，可实现文件 M 的完全恢复。图2为分布式云存储系统的示意图。单一传感器将感知数据通过中间的 n 个数据存储节点汇集于同一个汇集节点 DC 处。需要说明的是，对于这 n 个数据存储节点，要将任意模为 k 的子集都连接到一个数据收集接点，就应有 C_n^k 个汇聚节点，但为便于理解，图中仅以一个数据收集节点为代表。

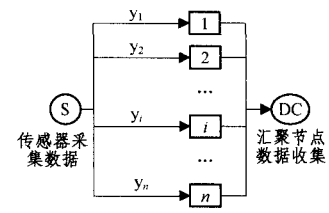

图2 分布式存储系统模型

以下是该云存储模型的数学描述。

设传感器 S 的感知数据存储在编号为 $1,2,\cdots,n$ 的云存储节点上，其传输数据包 M 被等分为 k 份，则每份的数据量为 M/k，分别标记为 $M=(m_1,m_2,\cdots,m_k)$。当数据块集合 M 编码之后，设生成的编码数据共有 n 个，可用向量表示为 $Y=(y_1,y_2,\cdots,y_n)$，每个编码数据 y_j 对应一个编码矢量，记作 $(g_{1j},g_{2j},\cdots,g_{kj})$。这样，可将系统模型简写为如下形式：

$$Y=(y_1,y_2,\cdots,y_n)=MG$$
$$=(m_1,m_2,\cdots,m_k)\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ & \cdots & \cdots & \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} \quad (1)$$

式中，矩阵 G 的维数为 $k\times n$，其列向量 $(g_{1j},g_{2j},\cdots,g_{kj})^{\mathrm{T}}$ 中的非零元素表示的是相应线性组合中用到的随机系数，这个列向量称为编码矢量[14]。

为有效减少数据传输过程中的加密、解密运算量，以满足无线传感网的数据加密需求，这里提出一种基于加密编码矢量的数据安全保障技术。需要说明的是，加密编码数据法是对需要存储的数据进行加密，用二元组可表示为 $(g_i,E_nC_{k_i}(y_i))$ 的形式；加密编码矢量法则主要是对数据的编码矢量进行加密，而非直接对数据本身进行加密，用二元组可表示为 $(E_nC_{k_i}(g_i),y_i)$ 的形式。为叙述方便，本文将加密编码矢量法的基本过程表示为如下形式：

$$g_i'=E_nC_{K_i}(g_i),1\leqslant i\leqslant n \quad (2)$$

由此可以看出，采用加密编码矢量方法不仅可以更好地保证欲传递数据的安全性，而且可有效减少需加密数据的数量。同时，随着无线传感网原始感知数据量的增大，加密编码矢量方法在数据的传输和计算处理方面所能带来的好处也就越大。

1.3 基于加密编码矢量方法的数据传输算法

对无线传感网感知数据进行加密编码矢量处理的算法过程可描述为如下主要步骤：

S1. 生成密钥，$\vec{K}=KeyGen(n,m)$。在密钥空间中，选择 n 个安全参数为 m 的密钥，设生成的密钥向量为 $\vec{K}=(K_1,K_2,\cdots,K_n)$。

S2. 将感知数据集合 M 使用网络编码算法进行编码，获得生成矩阵 G 和编码数据向量 Y，$(G,Y)=EnCode(M,n,k)$，其中，$G=(g_1,g_2,\cdots,g_n)$，$Y=(y_1,y_2,\cdots,y_n)$。每个云存储

节点 i 上存储的数据量为一个二元组(g_i, y_i)，其中 g_i 是编码矢量，y_i 是编码数据，且二者之间的关系是 $y_i = Mg_i$。

S3. 恢复原始数据时，所采用的解码算法可表示为 $M = DeCode((g_i, y_i)^k)$。该式表示，当输入任意 k 个数据存储节点上所存储的二元组(g_i, y_i)数据时，可通过求解线性方程的方法恢复出原始数据 M。

S4. 对编码矢量进行加密，所采用的加密算法形式为 $g_i' = E_n C_{K_i}(g_i)$。在密钥向量中选择 K_i 对编码矢量 g_i 进行加密，可得到密文 g_i'。

S5. 恢复编码矢量的解密算法为 $g_i = DeC_{K_i}(g_i')$，可使用密钥 K_i 对密文 g_i'进行解密，并得到恢复的明文 g_i。

下面证明上述算法的可行性。

已知：无线传感网的感知数据集是一个二元组(G, S)，其中 G 是有限有向图，S 是该图上唯一没有入边的节点。

求证：在无线传感网中，从源节点到非源节点 T 的流由一组通道构成(流中的通道称为忙通道)，且满足：

①基于忙通道的子网是无环的；

②除节点 S 和 T 外的任意节点，入边忙通道的数目等于出边忙通道的数目；

③S 出边忙通道数等于 T 入边的忙通道数。

源节点 S 出边忙通道的数目，称为流的容量；节点 T，称为流的汇聚节点；对于网络(G, S)中的所有节点 T，将从源节点到 T 的最大流容量记作 $\max_{flow}(T)$。

证明：由最大流-最小割(Max-Flow Min-cut)定理[15]可知，对于无线传感通信网，其线性码多播(linear code multicast)就是对网络中任意节点 X 赋予向量空间 $v(X)$并对任意通道 XY 赋予向量 $v(XY)$的过程，且存在

①$v(S) = \Omega$，Ω 为域上的 d 维向量空间；

②对任意通道 XY，存在 $v(XY) \in v(X)$；

③赋值到 T 的出边上的向量，是赋值到 T 的入边上的向量的线性组合；

④对网络中的任意非源节点集合 $\wp$，存在

$$\langle \{v(T): T \in \wp\} \rangle = \langle \{v(XY): X \notin \wp, Y \in \wp\} \rangle \tag{3}$$

式中，符号“〈〉”表示线性扩张。证毕。

1.4 加密编码矢量数据的存储和读取

采用加密编码矢量法对无线传感网感知数据进行存储，其过程可描述为：

S1. 设原始感知数据信息集合为 M，将其编码为 n 个二元信息组(g_i, y_i)；

S2. 对于每个二元组，依式(2)，使用密钥 K_i 进行编码矢量加密，即 $g_i' = E_n C_{K_i}(g_i)$；

S3. 将加密后的密文和编码数据组成新的二元组(g_i', y_i)；

S4. 将加密过的二元组发送到云存储节点 i 上，实现数据的安全存储。

对加密编码矢量数据的读取过程可以描述为：

S1. 随机选择 k 个云存储节点；

S2. 从每个云存储节点处下载加密的二元组数据(g_i', y_i)；

S3. 利用解密算法，获得密钥集；

S4. 对编码矢量进行解密，获得解密的编码矢量；

S5. 解码，获得数据的明文二元组(g_i, y_i)；

S6. 输出结果，获得数据明文。

1.5 加密编码矢量法的性能分析

基于加密编码矢量方法，可降低无线传感网因数据加密而带来的传输性能损失。因此，这里从理论层面来分析无线传感网数据在存储、读取和数据操作等过程的主要性能。

(1)考虑对传感器感知数据直接进行加密。①存储过程中，原始数据会被先加密成密文，然后再使用线性网络编码算法执行编码，因只需执行一次对原始数据的加密，其加密数据量为 kp 比特；②读取过程中，先由编码数据和编码矢量解码为密文，再由密文经解密算法恢复成明文，这一过程只需执行一次解密算法，其数据量同为 kp 比特；③因加密算法的扩散特性，修改数据至少会导致 nk^2 次乘法计算，且此过程需执行一次解密运算与一次加密运算，数据量为 kp 比特。

(2)考虑利用加密编码数据方法加密传感器感知数据信息。①存储过程中，需对每个存储节点的编码数据进行加密，加密数据量为 np 比特；②读取过程中，因只需对被选中的 k 个数据存储节点的编码数据进行解密，故数据量为 kp 比特；③修改数据过程中，需增加的计算量与数据操作集 ΔY 中的非零分量有关，最差情况下为 np 比特。

(3)考虑加密编码矢量法加密。这一过程与加密编码数据的加密方法计算过程类似，故在存储、读取和修改数据的过程中，需增加的加密数据量分别为 nu、ku 和 nu 比特。

三者分析结果的比较如表 1 所列。

表 1　3 种加密方法的性能分析

类型	加密原始数据	加密编码数据	加密编码矢量
存储	$E_nC(kp)$	$E_nC(np)$	$E_nC(nu)$
读取	$DEC(kp)$	$DEC(kp)$	$DEC(ku)$
修改	$E_nC(kp)+nk^2$	$E_nC(np)$	$E_nC(nu)$

由于 $n = \alpha k$ 且 $\alpha > 1$，因此加密编码数据法需加密的数据量为：

$$np = \alpha kp > kp \tag{4}$$

这说明，加密编码数据方法的性能要低于加密原始数据方法的性能。

对加密原始数据法和加密编码矢量法来说，因

$$\frac{kp}{\alpha ku} = \frac{p}{\alpha u} \tag{5}$$

为使加密编码矢量法的性能大于加密原始数据法，需

$$\frac{p}{\alpha u} > 1 \Leftrightarrow \alpha < \frac{p}{u} \tag{6}$$

故而可知，当 $\alpha < \frac{p}{u}$ 时，加密编码矢量法的性能将优于传统加密方法。

2 数据存储的安全性

在云存储系统中，设攻击者 A 随机选择存储数据生成矩阵 G 的一个 $k \times k$ 子阵，以其能够成功恢复出原始数据的概率的一半为标准，即

$$S(G) = x \mid P_{Y \to M}\{X \leqslant x\} \geqslant \frac{1}{2} \tag{7}$$

式中，$P_{Y \to M}\{X = x\} = p$ 表示经过 x 次矩阵乘法运算，可由编码数据 Y 成功恢复出数据 M 的概率。

为此，需进一步说明基于加密编码矢量法的传感器数据传输的安全性。设攻击者 A 所采用的攻击算法为穷举法：

S1. A 随机选择生成矩阵 $G(k, q)$中的一个子阵 B；

S2. A 在编码数据 Y 的所有子集中按序选取一个 Y_k^1；

S3. 计算 Y_k^1B，若 $Y_k^1B=M$，则攻击成功，又

$$p=\frac{1}{|G(k,q)|} \tag{8}$$

对于一般线性矩阵 $G(k,q)$，其阶等于

$$\prod_{i=0}^{k-1}q^i(q^{(k-i)}-1) \tag{9}$$

那么，将式(9)代入式(8)，则可得

$$p=\frac{1}{\prod_{i=0}^{k-1}q^i(q^{(k-i)}-1)} \tag{10}$$

由式(7)可知，欲使成功的概率大于$\frac{1}{2}$，则需满足

$$P_{Y\to M}\{X\leqslant x\}=x\,|\,p\geqslant\frac{1}{2} \tag{11}$$

可以看出，对于一个 $k\times k$ 阶、元素值随机取自有限域 $G(q)$ 的生成矩阵 G，由式(7)知

$$S(G)\geqslant\frac{1}{2p}=\frac{\prod_{i=0}^{k-1}q^i(q^{(k-i)}-1)}{2} \tag{12}$$

一般情况下，该式的计算结果可达 10^n 级，也就表明安全性较高。

3 实例与讨论

3.1 实验测试平台

测试平台主要利用了实验室已有的测试环境，硬件配置如表 2 所列，软件包括操作系统 XP SP3 和 Matlab 711 等。

表 2 测试平台配置

序号	名称	规格型号
1	联想 T2900	Intel E7500 双核 2.93GHz/内存 2GB/硬盘 320GB 7200 转
2	HP 工作站	Intel Xeon E5506 4 核 2.13GHz/内存 16GB/硬盘 1TB 1 万转
3	路由器	上传速率 128KB/s，下载速率 240KB/s
4	传感网	Crossbow 公司的 MIB520 采集板、Micaz 节点和 TinyOS 嵌入式系统

实验中，采用汇聚节点位置固定的方式，利用 MIB 520 采集板与各数据处理单元(本处为联想 T2900 客户端)相连，对传感器的感知数据进行实时收集和处理；各传感器沿作物垄畦田埂等距布置。同型 Micaz 节点在电路板印制、元器件点焊和电池电量的差异，会导致不同节点之间的射频信号收发存在差异。为此，本文对域中各汇聚节点的 RSS 观测值分别测量 10 次后求平均值，以期抵消这些不利因素的影响。图 3 给出了设备在田间实验的工作情况。

图 3 实验装置布设情况

3.2 安全性测试

实验中，利用式(12)，取 $q=7$，分别计算从 $k=10$ 到 $k=13$ 的值。各安全标准值的计算结果如表 3 所列。

表 3 $q=7$ 时的安全标准值

	k=10	k=11	k=12	k=13
S(G)	1.4×10^{84}	7.6×10^{101}	2.1×10^{121}	2.7×10^{142}

可以看出，表中各值数量级非常大，采用现代计算模型基本无法求解，说明基于网络编码的加密编码矢量方法是安全的，因而具有较高的安全性，可有效实现云存储节点上数据信息的安全性存储。

3.3 传输性能测试

为使测试结果更为可信，这里选择对面积大小为 100m×100m 的田间常规气象和田间参数进行实时采集和延时加密传输，包括风向、风速、温度、湿度、气压、雨量、大气压力、日照时数、土壤温湿度等，测试结果数据如表 4 所列。

表 4 远程和本地传输存储的平均总时间比重

文件大小(MB)	本地加密存储时间(ms)	远程加密存储时间(ms)	平均时间差(ms)	平均时间差/本地存储时间(%)
2.29	22495	24980	2485	11.05
4.36	40409	44916	4507	11.15
11.8	97703	110503	12800	13.10
25.1	206288	233622	27334	13.25
49.3	422431	466001	43570	10.31
70.8	620755	679739	58984	9.50

测试结果表明：①远程存储时间与本地网络的存储时间差较小，所占的总比重不大，对远程网络数据的影响在可接受范围内；②随着传输数据量的增加，本地存储与异地远程存储所占的时间比重在逐步下降，表明两者的存储时间在逐步贴近；③对于大数据量来说，由于使用了专业的云服务公司高性能存储设备，存储效能可以得到较好体现，如数据量从49.3MB增长到 70.8MB 时，存储效率从 10.31%下降为9.50%。

结束语 (1)无线传感网有望在现代精准农业生产过程中得到更为广阔的应用，在大田环境参数监测过程中，由云节点、域和主控节点所构成的监测体系是一种高效的云存储无线传感网感知结构；

(2)基于加密编码矢量方法，不仅可以较好地保证无线传感网感知数据传输的安全性，还可以有效减少原始数据的加密运算量，从而达到降低无线传感网传输带宽占用率、减少占用传感网计算资源的目的；

(3)农业生产过程中影响作物综合产出效益的影响因素多样，仅靠无线传感网通过环境因子的监测和反馈控制难以完全实现农业高效增产的目标，往往需要通过对农业生产的机械装备、农艺措施和作物性状等进行多信息融合分析，这也是本文开展后续工作的一个重要方向。

参 考 文 献

[1] Archila J F, De Castro S Z, Becker M. Technical Feasibility and Conceptual Design Applied to a Robotic Platform Embedded Sensing System Used in Precision Agriculture Engineering[C]// 22nd International Congress of Mechanical Engineering (COBEM 2013). Ribeirão Preto, SP, Brazil, 2013: 1417-1427

[2] 常超，鲜晓东，胡颖. 基于 WSN 的精准农业远程环境监测系统设计[J]. 传感技术学报，2011，24(6)：879-883

[3] 纪建伟，丁皓，李征明，等. 基于无线传输的稻田灌溉监控系统[J]. 农业工程学报，2013，29(S1)：52-59

[4] 张丹，王建华，吴玉华. 物联网技术在农业温室大棚中的应用研究[J]. 安徽农业科学，2013，41(7)：3218-3219，3246

[5] 徐焕良，张灏，沈毅，等. 基于低功耗传输方法的设施花卉环境监测系统[J]. 农业工程学报，2013，29(4)：237-244

[6] 张猛，房俊龙，韩雨. 基于 ZigBee 和 Internet 的温室群环境远程

监控系统设计[J]. 农业工程学报,2013,29(S1):171-176
[7] Liu Jian-qi, Wang Qin-ruo, Wan Jia-fu, et al. Towards Key Issues of Disaster Aid based on Wireless Body Area Networks [J]. KSII Transactions on Internet & Information Systems, 2013,7(5):1014-1035
[8] 吕军,孙微涛,李彤. 基于栅格分簇的无线传感器网络路由协议[J]. 计算机工程,2014,40(2):97-101
[9] Ji Sai, Sun Ya-jie, Shen Jian. A Method of Data Recovery Based on Compressive Sensing in Wireless Structural Health Monitoring[J]. Mathematical Problems in Engineering, 2014, 2014(1): 1-9
[10] De Souza Evandro, Nikolaidis Ioanis. An exploration of aggregation convergecast scheduling[J]. Ad hoc Networks, 2013, 11 (8):2391-2407
[11] Liu An, Ning Peng, Wang Chun. Lightweight remote image management for secure code dissemination in wireless sensor networks[C]// IEEE the 28th Conference on Computer Communications. Rio de Janeiro, Brazil, 2009:1242-1250
[12] Weatherspoon H, Kubiatowicz J D. Erasure coding vs. replication: A quantitative comparison[C]// Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS 2002). MIT Faculty Club, Cambridge, MA, USA, 2002:328-337
[13] Gu Ren-tao, Zhang Lin, Ji Yue-feng. Secure and efficient metro-access network using network coding[C]// 2011 International Conference on Information Photonics and Optical Communications (IPOC). Jurong West, 2011:1-4
[14] Boykov Y, Kolmogorov V. An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2004, 26(9):1124-1137

(上接第 367 页)

[2] Suo X, Zhu Y, Owen G S. Graphical passwords: A survey[C]// 21st Annual Computer Security Applications Conference. IEEE, 2005:472
[3] Aviv A J, Gibson K, Mossop E, et al. Smudge attacks on smartphone touch screens[C]// Proceedings of the 4th USENIX Conference on Offensive Technologies. USENIX Association, 2010: 1-7
[4] Von Zezschwitz E, Koslow A, De Luca A, et al. Making graphic-based authentication secure against smudge attacks[C]// Proceedings of the 2013 International Conference on Intelligent user Interfaces. ACM, 2013:277-286
[5] Kim S, Yi H, Yi J H. FakePIN: Dummy Key Based Mobile User Authentication Scheme[M]// Ubiquitous Information Technologies and Applications. Springer Berlin Heidelberg, 2014:157-164
[6] Kim H W, Kang A, Barolli L, et al. Efficient locking scheme with OPOF on smart devices[M]// Advances in Computer Science and its Applications. Springer Berlin Heidelberg, 2014:369-378
[7] Andriotis P, Tryfonas T, Oikonomou G, et al. A pilot study on the security of pattern screen-lock methods and soft side channel attacks[C]// Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2013:1-6
[8] Airowaily K, Alrubaian M. Oily residuals security threat on smart phones[C]// 2011 First International Conferenceon Robot, Vision and Signal Processing(RVSP). IEEE, 2011:300-302
[9] Tari F, Ozok A, Holden S H. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords[C]// Proceedings of the Second Symposium on Usable Privacy and Security. ACM, 2006:56-66
[10] Schaub F, Deyhle R, Weber M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms[C]// Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia. ACM, 2012:13
[11] Wu T S, Lee M L, Lin H Y, et al. Shoulder-surfing-proof graphical password authentication scheme[J]. International journal of information security, 2014, 13(3):245-254
[12] Chakraborty N, Mondal S. SLASS: Secure login against shoulder surfing[M]// Recent Trends in Computer Networks and Distributed Systems Security. Springer Berlin Heidelberg, 2014: 346-357
[13] Hirotaka N. Reassessing current cell phone designs: using thumb input effectively[C]// Extended Abstracts on Human Factors in Computing Systems(CHI'03). ACM, 2003:938-939
[14] Jermyn I, Mayer A, Monrose F, et al. The design and analysis of graphical passwords[C]// Proceedings of the 8th USENIX Security Symposium. 1999:1
[15] Wiedenbeck S, Waters J, Birget J C, et al. PassPoints: Design and longitudinal evaluation of a graphical password system[J]. International Journal of Human-Computer Studies, 2005, 63(1): 102-127
[16] Bicakci K, Atalay N B, Yuceel M, et al. Towards usable solutions to graphical password hotspot problem[C]// 33rd Annual IEEE International Computer Software and Applications Conference, 2009(COMPSAC'09). IEEE, 2009:318-323
[17] Shadmehr R, Brashers-Krug T. Functional stages in the formation of human long-term motor memory[J]. The Journal of Neuroscience, 1997, 17(1):409-419
[19] Von Zezschwitz E, Koslow A, De Luca A, et al. Making graphic-based authentication secure against smudge attacks[C]// Proceedings of the 2013 International Conference on Intelligent User Interfaces. ACM, 2013:277-286
[20] Taekyoung K, Sarang N. TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems[J]. Computers & Security, 2014(42):137-150
[21] De Luca A, Von Zezschwitz E, Nguyen N D H, et al. Back-of-device authentication on smartphones[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013:2389-2398
[22] Li K A, Baudisch P, Hinckley K. Blindsight: eyes-free access to mobile phones[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008:1389-1398