基于 Strand Space 的移动计算安全协议设计与正确性证明*)

许 峰[1,2] 高晓春[1] 黄 皓[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[1]
(河海大学计算机及信息工程学院 南京 210098)[2]

摘 要 安全协议对移动计算的安全性质起着决定作用。根据移动计算网络环境的特点,参照安全协议设计准则,以移动银行应用为背景设计了一个移动计算安全协议——MB协议,并基于 Strand 空间理论给出了正确性证明。

关键词 串空间,安全协议,形式化分析,密码体制,移动计算

Design and Correctness Proof of a Security Protocol for Mobile Computing

XU Feng[1,2] GAO Xiao-chun[1] HUANG Hao[1]
(State Key Lab. for Novel Software Technology, Nanjing University, Nanjing 210093, China)[1]
(College of Computer & Information Engineering, Hohai University, Nanjing 210098, China)[2]

Abstract The security protocol, which is a crucial basis in mobile computing, determines the security properties or even the fate of whole system. Therefore, investigated the runtime environment of mobile banking systems, studied the design and analysis methods of security protocols, and hereby proposed a security protocol for mobile computing——the MB-protocol. Discussed the important designing technologies used in MB protocol. Then gave a rigorous proof of correctness MB protocol based on strand space model.

Keywords Strand space, Security protocol, Formal analysis, Cryptography, Mobile computing

1 引言

移动计算网络是用户计算机可以在网内随意移动的计算机通信网络,用户可以在无线网络覆盖的任何地方随时发送和接收各种数据信息,而且可以在不同地区(甚至不同国家)之间进行漫游。与一般的有线网络相比,移动网络的安全性要求更高,主要表现在:无线电波自由传播,易被窃听,需要更复杂的加密技术;用户移动范围广,必须有一网管中心负责用户移动性管理、网络安全管理、数据库管理,包括用户注册和认证、计费、用户位置登记、用户漫游管理、越区切换等;用户终端有一定的计算能力和存储能力,它可能通过有线或无线方式接入因特网进行网页浏览、电子邮件收发,利用文件传输协议进行文件传输、加入新闻讨论组、接收多媒体视频服务以及进行电子交易和电子签定合同等因特网业务。

2 相关工作和进展

"移动银行"作为移动计算网络提供的一项电子商务服务,通过移动计算网络将客户手机连接至银行,利用手机界面直接完成各种金融理财业务。移动银行虽然具有传统商业银行无法比拟的优势,但是同其他新鲜事物的发展规律一样,移动银行的发展也存在许多困难和制约因素,其中最为突出的是安全机制不够健全。与网上银行一样,安全问题是人们最关心的问题。资金和货币的电子化,很容易使银行在转帐、交易、支付等服务过程中产生各种风险。无论是银行,还是企业或个人,如果没有足够的安全保障,是根本不会使用这一服务的。因此,要求在实施移动银行解决方案时,必须考虑交易过程中所涉及的各个方面、环节的安全性,必须采用比一般的信息增值服务高得多的安全保障机制,包括信息收发的保密性、完整性、不可抵赖性、公平性等。

迄今,针对移动通信系统以及个人通信系统设计了许多认证与会话钥建立协议[1-4],这些协议主要采用对称钥加密算法和杂凑算法,利用随机数挑战进行认证。若把这类协议直接用于移动计算网络环境,有一定的局限性,这主要表现在移动计算环境中的用户终端有一定的计算与存储能力,它可以接入因特网进行诸如网页浏览、电子商务、视频点播等业务,而不只局限于话音业务。同时,对于一个全球移动计算网络来说,要进行可靠的认证与支付,需要利用公钥基础设施。

本文汲取以往安全协议设计的经验,遵照安全协议的设计准则,以移动银行应用为背景,设计了一个适合于移动计算网络环境的安全协议—— MB(Mobile Banking)协议,并使用 Strand 空间理论进行周密细致的形式化分析,证明了其能实现期望的安全目标。

3 协议设计

3.1 设计条件

移动银行协议运行在移动通信环境中,由于其具有开放信道等特点,必须采用密码技术。移动网络中用户和访问网的信息交换会耗费较多时间,如何减少信息交换的次数及中间处理过程,是移动安全协议需要考虑的主要因素。

现在大多数移动设备,如手机、个人数字助理(PDA)等,其硬件一般较为简单,CPU 速度慢、内存少,电池容量也有限,所以用于常规安全认证的一些复杂运算应尽量避免使用。

*)本课题得到国家自然科学基金(60473091)和国家"八六三"高技术研究发展计划项目基金(2007AA01Z409)资助。许 峰 博士研究生,主要研究方向为信息安全和分布式计算;高晓春 博士研究生,主要研究方向为网络安全;黄 皓 教授,博士生导师,主要研究领域为网络安全。

而私钥算法在加、解密中运算速度快，应是移动安全协议采用的主要技术。

用户在申请开通移动银行业务时，验证银行的数字证书，领取银行颁发的 STK 卡，其中含有银行公钥。以后用户就利用 STK 卡提供的菜单进行操作，完成移动银行业务。同时，银行在验证用户的合法身份后，会为其申请一张合法的数字证书。在发给用户的 STK 卡中存有用户私钥，银行保存对应的公钥。这两对公私钥对是完成协议的必要前提，也是保证协议可追究性的基础。

3.2 功能及性能要求

移动银行安全协议首先要能保证交易的安全性，即，秘密性、认证性，完整性，以及可追究性，并能有效抵抗已知攻击；其次，协议应具有较高的效率，以便在手机受限的计算环境中能快速运行；最后，移动银行协议中的消息传递次数要尽可能少。

本文提出的 MB 协议在满足交易安全性的前提下，尽可能采用高效的适合移动设备计算的算法，以提高协议运行效率。同时，协议允许一个用户在多家银行开户，由移动短信中心负责将交易短信分发到各家银行，也是为实现一卡通用所做的一个尝试。

3.3 协议描述

3.3.1 符号说明

C(Customer)：手机用户标识(如帐号)；

B(Bank)：银行标识(如行号)；

S(Server)：移动短信服务中心标识；

k_1，k_2：新产生的随机会话密钥；

K_C^{-1}：手机用户的签名私钥；K_B^{-1}：银行的签名私钥；

K_C：手机用户的公钥；K_B：银行的公钥；

K_{CS}：手机用户与移动短信中心共享的密钥；

K_{BS}：短信中心与银行共享的密钥；

$\{m\}_k$表示消息 m 用密钥 k 加密；$\{m\}_{k^{-1}}$ 表示消息 m 用私钥 k^{-1} 签名。

$\{m_1, m_2\}$表示消息 m_1 和 m_2 串联后构成的新消息。

$h(m)$表示对 m 进行 Hash 运算，其值为 m 的摘要。

req：表示交易请求。

res：表示银行响应结果，可以是业务处理成功，也可是处理失败及原因。

3.3.2 协议形式化规则描述

如果将短信中心视为传输介质的一部分，仅考虑手机和银行两方参与者，则可将“手机用户→移动短信中心→银行→移动短信中心→手机用户”的协议工作流程简化为“手机用户→银行→手机用户”，进而得到 MB 协议的形式化描述如下：

$C \rightarrow B: \{req, \{h(C,B,req,k_2)\}_{K_C^{-1}}\}_{k_1}, \{k_1,k_2\}_{K_B}$

$B \rightarrow C: \{res, k_1, \{h(B,C,res)\}_{K_B^{-1}}\}_{k_2}$

由于 MB 协议涉及到移动设备，因此要尽可能减少移动设备上的计算量。协议中先取消息摘要，再进行运算量较大的签名运算。这样既能保证消息的完整性，又能满足可追究性的要求。数字信封$\{k_1,k_2\}_{K_B}$中的随机密钥 k_1，k_2 都由手机端产生，虽然多产生一个随机数会增大手机端的开销，但这样银行端就无需再用一个数字信封包装新密钥发给手机端，从而使手机端减少了一次耗时的公钥解密运算。显然，这样可以降低手机端的总计算量。协议将公钥加密和对称加密结合，公钥加密用于传递对称密钥，对称加密用于保护协议消息主体。考虑到在运算速度上公钥加密要远低于对称加密，这样做既可以获得足够的安全性，又能加快协议执行的速度。

MB 协议中，在移动端发送消息时，计算量较大的签名运算仅对消息摘要进行一次，而消息摘要较短，且长度固定，其余的密码运算是速度很快的分组密码加密和运算简单的公钥加密。移动端验证时，只做一次分组密码解密、一次公钥加密验证数字签名、一次求消息摘要运算，计算量都是有限的。因此，移动端的计算量得到了有效控制。

另外，协议的交易请求消息要比应答消息多一个数字信封，对称加密部分的结构、内容和长度也不相同，从而使它们的消息结构存在显著差别，这种非对称的消息结构是抵抗重放攻击的有效手段之一。攻击者将无法使用反射攻击，即不能把交易请求消息当作应答消息发送手机端，反之亦然。

4 基于 Strand 空间理论的 MB 协议分析

1998 年，Thayer，Herzog 和 Guttman 提出了 Strand 空间理论[5]，把协议的描述和目标安全属性都转化为图的结构，有利于借助图的理论和算法对协议进行分析和验证。Strand 空间模型理论代表了当前安全协议形式化验证的发展方向，有着良好的使用效果。

4.1 Strand 空间理论的基本概念

本节介绍 Strand 空间理论。首先介绍 Strand 空间理论的基本概念：项(terms)、串(strand)、串空间(Strand Space)以及簇(Bundles)，随后给出攻击者模型的形式化描述。

4.1.1 项与子项关系

定义一个集合 A，其中的元素称为项(terms)，表示协议各方可能交换的消息。文本项(代表原子消息)集记为 T，密钥项集记为 K，且 T 与 K 不相交。T 和 K 都是原子项，项可由原子项经过级连、加密得到。

定义 1 子项关系$\sqsubset$：

(1) 若 $t \in T, a \sqsubset t$ 当且仅当 $a = t$；

(2) 若 $k \in K, a \sqsubset k$ 当且仅当 $a = k$；

(3) $a \sqsubset \{g\}_k$，当且仅当 $a \sqsubset g$ 或 $a = \{g\}_k$；

(4) $a \sqsubset gh$，当且仅当 $a \sqsubset g$ 或 $a \sqsubset h$ 或 $a \sqsubset gh$；

定义 2 有符号项是一个有序对$\langle \sigma, a \rangle$，$a \in A$，$\sigma$ 为＋或－，记作$+a$ 或$-a$，$+a$ 表示发送项 a；$-a$ 表示接收到项 a。$(\pm A)^*$ 是有符号项的有限序列的集合，表示为$\langle \langle \sigma_1, a_1 \rangle, \cdots, \langle \sigma_n, a_n \rangle \rangle$。

4.1.2 Strand 与 Strand 空间

Strand 是协议参与方的事件序列。对于合法参与者，每个 Strand 是一系列接收和发送的消息，代表该参与者在一次特定协议执行中的行为。攻击者 Strand 是攻击者可能发送和接收的消息序列。

定义 3 Strand 空间是包含各种合法主体 Strand 和攻击者 Strand 的集合 Σ 及定义在其上的映射 $tr: \Sigma \rightarrow (\pm A)^*$：

(1) 节点是一个有序对$\langle s, i \rangle$，$s \in \Sigma$，i 是满足 $1 \leqslant i \leqslant length((tr(s)))$的整数。每个节点$\langle s, i \rangle$属于唯一的 Strand。节点的集合记为 N。

(2) 如果 $n = \langle s, i \rangle \in N$，那么 $index(n) = i$，$strand(n) = s$。定义 $term(n) = tr(s)_i$，为 Strand s 的迹中第 i 个有符号项。类似地，$uns_term(n)$是 $tr(s)_i$ 的无符号部分。对于项 a，用 $node(+a)$或 $node(-a)$表示它所在的节点。

(3) $n_1, n_2 \in N$，那么 $n_1 \rightarrow n_2$ 表示 $term(n_1) = +a$，$term(n_2) = -a$，即节点 n_1 发送的消息 a 由 n_2 接受，因此它们的 Strand 之间就存在一个因果连接。

(4) $n_1, n_2 \in N$，那么 $n_1 \Rightarrow n_2$ 表示 n_1, n_2 属于同一个 Strand，且 $index(n_1) = index(n_2) - 1$，即 n_1 是 n_2 在 Strand 中的直接前驱。

(5)无符号项 t 出现在节点 n 上，当且仅当 $t \sqsubset term(n)$。

(6)无符号项 t 从节点 n 产生，当且仅当 $term(n)$ 的符号为正；$t \sqsubset term(n)$；且对于同一个 Strand 上任何先于 n 的节点 n'，$t \not\sqsubset term(n')$。

(7)无符号项 t 从节点 n 惟一产生，当且仅当惟一的节点 n 产生 t。若 t 在某个 Strand 空间中惟一产生，t 就可以作为现值或会话密钥。

所以，Strand 空间构成一个有向图 (N, E)，N 是节点集合，边 $E = (\rightarrow \cup \Rightarrow)$，可以把边看作节点之间的因果依赖关系。

4.1.3 Bundle

Bundle 是 Strand 空间的一部分，代表协议可能的运行模式。

定义 4 设 C 是边的集合，N_C 是由与 C 中边相连的节点集合。C 是 Bundle，如果

(1) C 是有限集；

(2) 如果 $n_1 \in N_C$，且 $term(n_1)$ 的符号为负，那么有唯一的节点 n_2，满足 $n_2 \rightarrow n_1 \in C$；

(3) 如果 $n_1 \in N_C$，且有 $n_2 \Rightarrow n_1$，那么 $n_2 \Rightarrow n_1 \in C$；

(4) C 是无环的。

如果节点 $n \in N_C$，则称 n 在 bundle C 中，记为 $n \in C$；若 Strand s 的所有节点都在 N_C 中，则称 s 在 C 中。

4.1.4 攻击者模型

Strand 空间理论建立了攻击者行为模型，对于攻击者的一些基本攻击进行了形式化的描述。攻击者能力主要由两方面因素描述：一是攻击者所掌握的密钥集，二是描述攻击者由他所获得的消息产生新消息的能力。其中攻击者所掌握的密钥集由 Kp 表示，攻击者的基本行为用下面的一个攻击者的迹的集合 Strand P 来表示：

(1) M[t]. 产生原子文本消息：$\langle +t \rangle$，$t \in T$。

(2) F[g]. 接收消息：$\langle -g \rangle$。

(3) T[g]. 接收并多次发送消息：$\langle -g, +g, +g \rangle$。

(4) C[g,h]. 级连收到的消息：$\langle -g, -h, +gh \rangle$。

(5) S[g,h]. 分割收到的消息：$\langle -gh, +g, +h \rangle$。

(6) K[k]. 发送密钥：$\langle +k \rangle$，$k \in K_P$，K_P 表示攻击者知道的密钥集合，包括所有的公钥、他所有的私钥及与 x 的共享密钥 Kpx，或者通过密码分析得到的密钥。

(7) E[k,h]. 加密消息：$\langle -K, -h, +\{h\}_K \rangle$。

(8) D[k,h]. 解密消息：$\langle -K^{-1}, -\{h\}_k, +h \rangle$。

攻击者 Strand 集精确地描述了攻击者的能力。

Strand 空间模型理论的详细描述可见文献[5]。

根据移动银行协议的设计要求，MB 协议的正确性主要体现在两个方面。

(1)认证属性：当认证主体以某参数完成其协议后，被认证主体也必须以该参数参与协议运行。

(2)秘密属性：保护协议消息不被泄漏给未被授权的主体。

下面使用 Strand 空间理论证明 MB 协议的这两个安全性质。

用 Strand 证明协议的基本方法是：首先，在 bundle 中根据需要构造一个节点集；其次，考虑节点集的最小元属于哪一种 Strand；最后，对于其余 Strand，分情况判断该最小元是否属于这个 Strand。如果最小元属于该 Strand，说明协议有缺陷。

4.2 MB 协议的 Strand 空间

定义 5 一个存在攻击的 Strand 空间 (Σ, P) 是一个 MB Strand 空间，如果 Σ 是以下三个 Strands 的并集：

1)攻击者的 Strands $p \in P$。

2)用户 Strands $s \in$ Customer$[B, C, k_1, k_2, req, res]$，其迹为：

$\langle +\{\{req, \{h(C,B,req,k_2)\}_{K_C^{-1}}\}_{k_1}, \{k_1, k_2\}_{K_B}\}, -\{res, k_1, \{h(B,C,res)\}_{K_B^{-1}}\}_{k_2} \rangle$

其中 $C, B \in T, k_1, k_2 \in K$，Customer$[B, C, k_1, k_2, req, res]$ 是包含上述迹的所有 Strands 的集合。与此 Strand 关联的主体是手机用户 C。

3)银行 Strands $t \in$ Bank$[B, C, k_1, k_2, req, res]$，其迹为：

$\langle -\{\{req, \{h(C,B,req,k_2)\}_{K_C^{-1}}\}_{k_1}, \{k_1, k_2\}_{K_B}\}, +\{res, k_1, \{h(B,C,res)\}_{K_B^{-1}}\}_{k_2} \rangle$

其中 $C, B \in T, k_1, k_2 \in K$，Bank$[B, C, k_1, k_2, req, res]$ 是包含上述迹的所有 Strands 的集合。与此 Strand 关联的主体是银行 B。

已知一个 Σ 中 Strand s，可以根据它的迹唯一区分出攻击者的 Strand、用户 Strand 和银行 Strand。

4.3 认证属性的证明

MB 协议的主要功能之一是身份认证。在文献[7]中，Woo 和 Lam 把协议的认证目标转化成对应属性。对应属性是说当认证主体以参数 x 完成他的部分协议后，被认证主体也必须以参数 x 参与协议运行，并作为本次运行的发起者。

在 Strand 空间理论中，MB 协议的对应属性可描述为命题 1：

若 1) Σ 是 MB Strand 空间，C 是 Σ 中的一个 Bundle，s 是 Customer$[B, C, k_1, k_2, req, res]$ 中的一个 C-高度为 2 的用户 Strand。

2) $K_B^{-1}, K_C^{-1}, k_1, k_2 \notin K_P$。

3) $k_1 \neq k_2$，且 k_1, k_2 唯一产生于 Σ。

则 C 包含一个 C-高度为 2 的银行 Strand $t \in$ Bank$[B, C, k_1, k_2, req, res]$。

用户 Strand 如图 1 所示。对应属性的证明目标可以细分为：首先，存在一个发起者 Strand t；其次，证明发起者的身份为 n_1，即 $x = n_1$；最后，证明与 n_2 进行身份认证，即 $y = n_2$。为了证明方便，图 1 给出了用户 strand 的图形表示。下面通过 3 个引理分别证明 3 个目标：

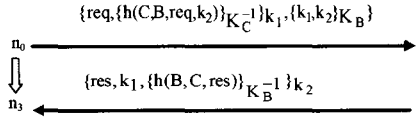

图 1 用户 Strand

引理 1 集合 $V = \{n \in C; k_1 \sqsubset uns\_term(n) \wedge \{k_1, k_2\}_{K_B} \not\sqsubset uns\_term(n)\}$ 至少有一个 $\leqslant$-minimal 节点 n_2，n_2 是常规节点，且符号为正。

证明：由于 $k_1 \sqsubset term\langle s, 1 \rangle = term(n_0)$，因此 k_1 产生于 n_0。由图 1 可知 $n_3 \in C, n_3 \in V$，所以 V 非空，那么 V 至少有一个 $\leqslant$-minimal 成员 n_2，其符号为正。n_2 能否出现在攻击者的 Strand p 上，有以下几种可能：

M · $tr(p)$ 的形式为 $\langle +t \rangle$，$t \in T$，但 $T \cap K = \phi$，而 $k_1 \in K$，所以 $t \neq k_1$，该情况不可能。

F • $tr(p)$的形式为$\langle -g\rangle$，没有符号为正的节点。

T • $tr(p)$的形式为$\langle -g,+g,+g\rangle$，正节点不是极小出现。

C • $tr(p)$的形式为$\langle -g,-h,+gh\rangle$，设$term(n_2)=+gh$。∵ k_1是简单的，∴ $k_1\subset g$或$k_1\subset h$，所以，正节点不是极小出现。

E • $tr(p)$的形式为$\langle -K,-h,+\{h\}_K\rangle$，设$k_1\subset\{h\}_K\wedge\{k_1,k_2\}_{K_B}\not\subset\{h\}_K$，∵$k_1\subset\{h\}_K, k_1\neq\{h\}_K$∴$k_1\subset h$，又$\{k_1,k_2\}_{K_B}\not\subset h$，∴正节点不是极小出现。

K • $tr(p)$的形式为$\langle +k\rangle, k\in K_P$，但$k_1\notin K_P$，故此情况不可能。

D • $tr(p)$的形式为$\langle -K^{-1},-\{h\}_k,+h\rangle$，若$k_1\subset h\wedge\{k_1,k_2\}_{K_B}\not\subset h$，由$h$的极小性，可设$\{k_1,k_2\}_{K_B}=\{h\}_K$，由自由加密假设，得$h=\{k_1,k_2\}, K=K_B$。故存在一个节点$m$，有$term(m)=K_B^{-1}$但$K_B^{-1}\notin K_P$，所以$K_B^{-1}$只能发自一个常规节点。但协议中没有哪个合法主体发送过K_B^{-1}。

S • $tr(p)$的形式为$\langle -gh,+g,+h\rangle$，不失一般性，设$term(n_2)=g, term(n_2)=h$的情况是对称的。∵$k_1\subset g\wedge\{k_1,k_2\}_{K_B}\not\subset g$，由$g$的极小性，可设$\{k_1,k_2\}_{K_B}\subset gh$，又$\{k_1,k_2\}_{K_B}$是简单的，∴$\{k_1,k_2\}_{K_B}\subset h$。记$U=\{m\in C: m\prec n_2\wedge gh\subset uns_term(m)\}$，因为$term(\langle p,1\rangle)=-gh$，故$\langle p,1\rangle\in U$，$U$非空，$U$至少有一个极小元$m_1$。

显然，m_1不可能在上述M，F，T，K型的攻击者Strand上。

S • $tr(p)$的形式为$\langle -gh,+g,+h\rangle$，若$gh\subset term(m_1)$，m_1是S型Strand p'上的一个正节点，则$gh\subset term(\langle p',1\rangle)$，$\langle p',1\rangle\prec m_1$，与$m_1$是$U$中极小元矛盾。

E • $tr(p)$的形式为$\langle -K,-h,+\{h\}_K\rangle$，若$gh\subset term(m_1)$，$m_1$是E型Strand p'上的一个正节点，则$gh\subset term(\langle p',2\rangle)$，$\langle p',2\rangle\prec m_1$，与$m_1$是$U$中极小元矛盾。

D • $tr(p)$的形式为$\langle -K^{-1},-\{h\}_k,+h\rangle$，若$gh\subset term(m_1)$，$m_1$是D型Strand p'上的一个正节点，则$gh\subset term(\langle p',2\rangle)$，$\langle p',2\rangle\prec m_1$，与$m_1$是$U$中极小元矛盾。

C • $tr(p)$的形式为$\langle -g,-h,+gh\rangle$，若$gh\subset term(m_1)$，m_1是C型Strand p'上的一个正节点，则$gh=term(m_1), term(\langle p',1\rangle)=g=term(n_2)$，故$\langle p',1\rangle\prec\langle p',3\rangle=m_1\prec n_2$，与$n_2$是$V$中极小元矛盾。

因此，n_2不在攻击者Strand上，而在常规Strand上。

引理2 在t中，存在一个节点n_1在n_2之前，使得$\{k_1,k_2\}_{K_B}\subset term(n_1)$。

证明：如图2所示，k_1产生于n_0，且唯一产生于Σ。又$\{k_1,k_2\}_{K_B}\subset term(n_0)$，但$\{k_1,k_2\}_{K_B}\not\subset term(n_2)$，故$n_0\neq n_2$，∴$k_1$不产生于$n_2$，因此，在$n_2$所在的Strand t上，必有一节点n_1在n_2之前，使得$k_1\subset term(n_1)$，由n_2的极小性，得$\{k_1,k_2\}_{K_B}\subset term(n_1)$。

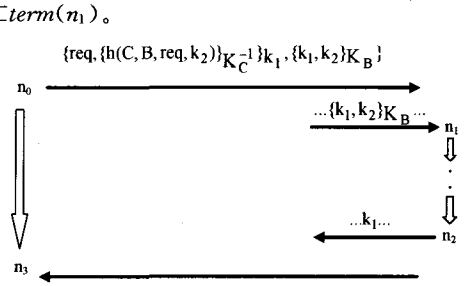

图2 节点n_1包含$\{k_1,k_2\}K_B$

引理3 常规Strand t是一个包含在C中的银行Strand，则t包含n_1和n_2。

证明：n_2是一个常规正节点，并且在节点n_1之后，而节点n_1包含形如$\{xy\}_k$的项。如果t是用户Strand，则在包含形如$\{xy\}_k$项的节点之后只能是负节点。但n_2是正节点，因此，t一定是一个银行Strand，n_1和n_2分别是t的第一个节点和第二个节点。由于t的最后一个节点包含在C中，它的C-高度一定是2。

根据引理2和引理3，命题1立即得证。

4.4 秘密属性的证明

下面证明协议中产生的密钥k_1, k_2是保密的。秘密属性在Strand空间理论中可以形式化描述为命题2：

若1)Σ是MB Strand空间，C是Σ中的一个Bundle，s是Customer$[B,C,k_1,k_2,req,res]$中的一个C-高度为2的用户Strand。

2) $K_B^{-1}, K_C^{-1}, k_1, k_2\notin K_P$。

3) $k_1\neq k_2$，且k_1, k_2唯一产生于Σ。

则对所有节点$m\in C$，当$k_1\subset term(m)$时，必有$\{k_1,k_2\}_{K_B}\subset term(m)$或者$\{res,k_1,\{h(B,C,res)\}_{K_B^{-1}}\}_{k_2}\subset term(m)$。

证明：设$\{res,k_1,\{h(B,C,res)\}_{K_B^{-1}}\}_{k_2}=v_3$。

考虑集合$F=\{n\in C: k_1\subset term(n)\wedge\{k_1,k_2\}_{K_B}\not\subset term(n)\wedge v_3\not\subset term(n)\}$。设$F$非空，则$F$至少有一个极小元。下面先证明这些极小元不是常规节点，再证明它们也不是攻击节点，因此F为空，命题得证。

设m是F的极小元，且是常规节点，则m的符号为正。在s中只有n_0的符号为正，但$\{k_1,k_2\}_{K_B}\subset term(n_0)$，所以$m$不在$s$上。又$k_1$唯一产生于$n_0$，∴$m$不在其他常规Strand $s'\neq s$上，故m不可能是常规节点。

F的极小元不是攻击节点的证明和引理1的证明极为相似，只是在考虑D型攻击者Strand时，要多考虑一种情况，即：$h=\{res,k_1,\{h(B,C,res)\}_{K_B^{-1}}\}_{k_2}, K=k_2$。这时，必须有一个节点$n$，有$term(n)=k_2$，但$k_2\notin K_P$，所以$k_2$只能发自一个常规节点。但协议中没有哪个合法主体发送过k_2。

综上所述，F只能为空，所以密钥k_1只能以协议规定的加密形式出现，因而是保密的。

密钥k_2的地位和k_1是等价的，其保密性的证明与k_1完全类同，不再赘述。交易请求req的秘密性证明也是类似的。

结束语 本文深入研究了移动计算网络的运行环境、安全协议的设计和分析方法及协议所需密码算法的安全性质，精心选择了一套包括分组密码、公钥密码、Hash函数和数字签名的密码算法。在此基础上设计了一个移动银行安全协议——MB协议，分析了设计协议时使用的重要技术，并和其他相关协议进行了比较。

然后基于Strand空间模型给出了严谨周密的正确性证明。MB协议的正确性主要体现在两个方面。认证属性：当协议主体以某参数完成协议后，被认证主体也必须以该参数参与协议运行；秘密属性：保护协议消息不会泄漏给未被授权的主体。从协议的分析过程中得到的结论是：MB协议实现了安全目标，能抵抗目前已知的攻击，且运行性能较优。

本文提出的MB协议是应用安全协议形式化方法进行设计和分析的一次有益尝试，对类似的移动计算协议的设计有一定的指导意义。该协议也易于在移动银行系统中实现，具

（下转第184页）

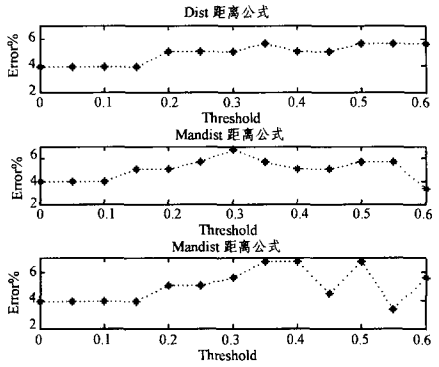

图 2 Wine Recognition Data 在 ε 在[0,0.6]之间,步长为 0.05,在三种不同范下式对应的误分率(其中距离的平均值为 $\bar{u}=0.6194$)

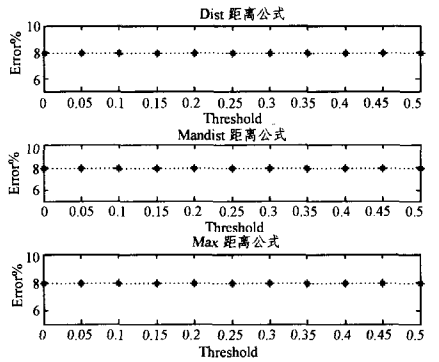

图 3 Letter Image Recognition Data 在 ε 在[0,0.5]之间,步长为 0.05,在三种不同范式下对应的误分率(其中距离的平均值为 $\bar{u}=0.5671$)

精度的影响。实验分析表明,基于邻域模型的初始聚类中心选择算法优于随机选择初始聚类中心和 CCIA 选择初始聚类中心算法,相对而言参数 ε 较小的时候聚类精度较高,效果较为理想。

参 考 文 献

[1] Han J, Kamber M. Data Mining: Concepts and Techniques. San Francisco, US: Morgan Kaufmann, 2001

[2] 张讲社,梁怡,徐宗本. 基于视觉系统的聚类算法. 计算机学报,2001,24(5):496-501

[3] 金阳,左万利. 一种基于动态近邻选择模型的聚类算法. 计算机学报,2007,30(5):756-762

[4] 张敏,于剑. 基于划分的聚类模型. 软件学报,2004,15(6):858-868

[5] 行小帅,潘进,焦李成. 基于免疫规划的 K-means 聚类算法. 计算机学报,2003,26(5):605-610

[6] Mac Q J. Some methods for classification and analysis of multivariate observation // Proceeding 5th Berkley Symposium. On Mathematical Statistics and Probability, 1967, I: 281-297 University of California Press. 1967, Xvii: 666

[7] Huang Z X. Extensions to the k-Means algorithm for clustering large data sets with categorical values. Data Mining and Knowledge Discovery, 1998, 2: 283-304

[8] Ahmad A, Dey L. A K-means clustering algorithm for mixed numeric and categorical data. Data & Knowledge Engineering, 2007, 63: 503-527

[9] Duda R O, Hart P E. Pattern Classification and Scene Analysis. John Wiley and Sons. NY, 1973

[10] Bradley P S, Mangasarian O L, Street W N. Clustering via concave minimization. In: M. C. Mozer, M. I. Jordan, T. Petsche, Eds. Advances in Neural Information Processing System, MIT Press, 1997, 9: 368-374

[11] Penā J M, Lozano J A, Larrañaga P. An empirical comparsion of four initalization methods for the K-means algorithm. Pattern Recognition Letter, 1999(20): 1027-1040

[12] Khan S S, Ahmad A. Cluster center initialization algorithm for K-means clustering. Patter Recognition Letters, 2004, 25: 1293-1302

[13] Lin T Y. Granular Computing on binary relations I: data mining and neighborhood systems. In: rough sets in knowledge discovery, Skoworn A and Pokowshi L(eds) Physica-Verlag, 1998: 107-121

[14] Yao Y Y. Relational interpretation of neighborhood operators and neighborhood systems. Information Sciences, 1998, 111 (198): 239-259

[15] Wu W Z, Zhang W X. Neighborhood operator systems and approximations. Information Sciences, 2002, 144(1/4): 201-217

[16] Hu Q H, Yu D R, Xie Z X. Neighborhood classifiers. Expert Systems with Applications, 2007(in Press)

[17] Meila M, Heckerman D. An experimental comparison of several clustering methods. Microsoft Research Report MSR-TR-98-06. Redomnd, WA, 1998

[18] Yang Y M. An evaluation of statistical approaches to text categorization. Journal of Information Retrieval, 1999, 1 (1/2): 67-88

(上接第 77 页)

有较好的应用价值。

参 考 文 献

[1] Gritzalis S, Spinellis D, Georgiadis P. Security protocols over open networks and distributed systems: formal methods for theiranalysis, design, and verification. Computer Communications, 1999, 22(8): 695-707

[2] Cervesato I, Durgin N A, Lincoln P D, et al. Relating strands and multiset rewriting for security protocol analysis // Proceedings of the 13th IEEE Computer Security Foundations Workshop. Cambridge, England, 2000: 35-52

[3] Thomas Y C W, Simon S L. A semantic model for authentication protocols // Proceedings of the 14th IEEE Symposium on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1993: 178-194

[4] Woo T Y C, Lam S S. A semantic model for authentication protocols // Proceedings of the IEEE Symposium on Research in Security and Privacy. Oakland, CA, 1993: 178-194

[5] Thayer F, Herzog J C, Guttman J D. Strand space: why is a security protocol correct // Proceedings of the 1998 IEEE Symposium on Security and Privacy. 1998: 160-171

[6] 范红,冯登国. 安全协议理论与方法. 北京:科学出版社,2003

[7] 卿斯汉. 安全协议 20 年研究进展. 软件学报,2003,14(10): 1740-1752

[8] Schneier B. Applied Cryptography 2nd Edition. New York: John Wileysons, 1996

[9] Halpern J Y, Fagin R. Modelling konwledge and action in distributed systems. Distributed Computing, 1989, 3(4): 159-179

[10] Marrero W, Clarke E, Jha S. Verifying security protocols with Brutus. ACM Transactions on Software Engineering and Methodology, 2000, 9(4): 443-487

[11] Stoller S D. A bound on attacks on payment protocols // Proceedings of the 16th Annual IEEE Symposium on Logic in Computer Science(LICS). Boston, Massachusetts, 2001: 61-70