一种适用于嵌套加密协议分析的强认证测试方法

宋巍涛 胡 斌
(信息工程大学 郑州 450001)

摘 要 认证测试是一种新型的在串空间模型基础上提出来的用于分析协议认证属性的形式化方法,该方法因简单实用而受到学者的广泛关注,但其不能分析协议中认证测试组件嵌套加密的情况,这极大地限制了它的应用范围。而现存的针对该局限性的改进方案,由于没有从本质上对串空间模型中关于消息项结构关系方面的语义进行完善,很难彻底突破认证测试的局限性。为此,通过在串空间模型中引入等价类、类组件、安全加密元及安全包裹元等概念,提高了串空间刻画消息项之间及内部结构关系的能力,并结合实例来阐明引入这些概念的必要性。在此基础上,提出一种可以分析测试组件嵌套加密的通用的认证测试方法,并从形式化证明与实例分析两方面验证了新测试方法的正确性与有效性。

关键词 安全协议,形式化分析,串空间,认证测试
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.1.035

One Strong Authentication Test Suitable for Analysis of Nested Encryption Protocols

SONG Wei-tao HU Bin
(Information Science and Technology Institute, Zhengzhou 450001, China)

Abstract Authentication test is a new type of analysis method of security protocols, which is proposed based on strand space model. It attracts a majority of scholars' attention because of its simple and practical, but it doesn't suitable for the analysis of nested encryption protocols. This greatly restricts the application of the method. Meanwhile, the existing improvement schemes are difficult to break through the limitation thoroughly on account of strand space's poor ability of reflecting the internal relations of terms. By introducing the definitions of equivalence class, class elements, security encryption item, and security encryption package, etc., this paper improved the strand space's ability of depicting the internal relations of terms. Then it put forward a general authentication test scheme which can be applied to anylize the nested encryption scenarios of authentication test element in the protocols. Furthermore, we verified the correctness and effectiveness of the new method from two aspects: formal proof and instance analysis.

Keywords Security protocol, Formal analysis method, Strand space, Authentication test

1 引言

安全协议的认证属性可以防止假冒、篡改、抵赖等攻击,实现身份认证、数据源和目标认证,并广泛应用于互联网密钥交换协议、电子商务协议等许多领域。但是目前缺乏一套成熟有效的安全性分析理论,协议的认证常常会存在各种漏洞,因此迫切需要一种形式化分析工具来对协议进行严谨的形式化分析,以检查协议的认证目标是否达到,是否存在安全缺陷或冗余等。

1998年,Fabrega、Herzog和Guttman提出的串空间模型[1]将安全协议形式化分析技术推向了一个新的高度,它简洁、严谨、直观,且具有一个开放的架构,可以将现有的密码协议形式化分析所用的许多方法与技术融合在一起[2]。2000年Guttman等人在串空间的基础上提出了一种用于证明协议认证属性的新方法,称之为认证测试[3]。该方法较串空间经典理论中构造集合、寻找集合最小元素的证明方法更为直观、简练,且实用性强,同时它还可指导协议设计[4-6]。其基本思想为:只有持有对应密钥的合法主体才能解读或者构造出认证测试所需的关键信息,即测试组件,从而达到认证对方存在的目的。在认证测试组件不能嵌套加密时,这种方法是正确的。但在认证测试组件可以嵌套加密时,认证主体可能在认证测试完成之前无意泄漏测试组件相关信息,使攻击者即使不知道解读或构造测试组件的相关密钥,也可以完成认证变换。为此,Guttman等人在提出认证测试定理时,要求测试组件不能嵌套加密,这虽然保证了认证测试的正确性,但却极大地限制了认证测试的应用范围。

2000年Perrig和Song在文献[7]中提出了认证测试的一个改进方案。该方案通过在原认证测试中用子项来替换组件,及增加限制条件等途径,在一定程度上避免了测试组件嵌套加密时因主体自身信息泄漏造成的认证测试定理不成立的

到稿日期:2014-02-06 返修日期:2014-04-09 本文受国家自然科学基金(61272041,61202491,61272488)资助。
宋巍涛(1989-),男,硕士,主要研究领域为密码学与信息安全,E-mail:weitaosong@163.com;胡 斌(1971-),男,教授,博士生导师,主要研究领域为密码学与信息安全。

情况。但该方案只考虑测试组件在认证主体源发结点的信息泄漏，忽略了其它节点也可能泄漏相关信息，因此只能应用于特定条件下的测试组件嵌套加密的情况。2006 年文献[8]对原认证测试中的主动测试进行了改进，同时定义了丛中正常(regular)密钥这个概念，并基于此改进了主动测试定理的条件，扩展了文献[7]中主动测试定理的应用范围，但文献[8]没给出相应的形式化证明。文献[9]通过实例对认证测试在测试组件嵌套加密时失效的原因进行了分析，并尝试对输入测试定理进行改进，以求扩大其适用范围，但文献[9]没有给出具体的改进方案。文献[10]在前人工作基础上，提出了一种新的认证测试改进方法，克服了原认证测试定理中测试组件不能嵌套加密的限制，同时有效地避免了上述文献改进方案的局限性。文献[11-14]对串空间模型中关于密钥方面的语义进行了丰富，引入了诚实函数、安全密钥等定义，但该改进方案没从本质上扩展串空间关于消息项内部结构的描述语言，因此在嵌套加密协议分析中仍具有很大的局限性。文献[15]针对认证测试模型的协议主体密钥的性质进行了研究，给出协议主体密钥在测试组件构造上的性质命题，在一定程度上适用于认证测试组件嵌套加密协议的认证属性分析。上述文献在本文统一称为认证测试类，它们虽然在一定程度上扩展了认证测试的应用范围，但本质上都是在原串空间模型基础上进行的改进，并没有涉及对串空间模型中有关消息项之间及内部结构关系方面的语义进行有效的完善，因此很难彻底突破认证测试的局限性，导致基于它们进行协议认证属性分析时，存在错误认证、实现上的冗余或认证不彻底等问题。

为此，本文通过首次在串空间模型中引入等价类、类组件、安全加密元及安全包裹元等概念，对串空间模型中有关消息项结构关系方面的语义进行了完善，提高了串空间刻画消息项之间及内部结构关系的能力，并以实例来阐明引入这些概念的必要性。在此基础上，提出了一种可以分析协议测试组件嵌套加密的通用的认证测试方法，称之为强认证测试方法，并对其进行了形式化证明。最后运用强认证测试方法对 SPLICE/AS 协议的认证属性进行了安全性分析，分别提出了该协议各角色认证上存在的问题，并且给出了相关的攻击实例，从而验证了强认证测试方法的有效性，同时也反映出本文提出的强认证测试方法不仅可以证明协议的认证性是否得到保证，还可以指导协议攻击实例的构造，并且协议越复杂，认证测试组件嵌套层数越多，该方法的分析效率越高。

2 预备知识

2.1 符号说明

文中所用标识意义如下：

A,B,S 表示主体；K_A 表示 A 的公钥；K_A^{-1} 表示 A 的私钥；K_{AB} 表示 A 和 B 之间的共享密钥；N_A 与 N_B 分别表示 A 和 B 产生的随机数；$\{m\}_K$ 表示消息 m 用密钥 K 加密形成的消息，其中 K 可以为公钥、私钥、对称密钥及杂凑密钥等各种密钥；m_1m_2 表示消息 m_1 与消息 m_2 的级联；P 表示攻击者所有可能获知的消息的集合，并假设任何主体的公钥都可以通过 PKI 机制安全、可靠地公开获得。

2.2 假设

(1)完善的加密前提：协议采用的密码系统是完美的，不考虑密码系统被攻破的情况，必须知道解密密钥才能解密加密数据；

(2)无加密项冲突：即若有 $\{m\}_K=\{m'\}_{K'}$，则一定可以推出 $m=m'$ 并且 $K=K'$；

(3)连接加密互斥：$m_1m_2\neq\{m_3\}_K$；

(4)原子不可拆分：$m_1m_2\notin T\cup K$，$\{m\}_K\notin T\cup K$。

2.3 基本知识

下面列出本文中用到的基本概念和引理，引理的具体证明参见文献[1,3]。

定义 1[1] 子项关系$\sqsubset$可以递归定义为满足下列关系的最小关系：(1)$m\sqsubset m$；(2)如果 $m\sqsubset m_1$，那么 $m\sqsubset\{m_1\}_K$；(3)如果 $m\sqsubset m_1$ 或者 $m\sqsubset m_2$，那么 $m\sqsubset m_1m_2$。当 $m\sqsubset m_1$ 且 $m\neq m_1$ 时，称 m 为 m_1 的真子项。

定义 2[1] 如果结点 $n=\langle s,i\rangle$ 为正，$t\sqsubset term(n)$，且对于任何 $j<i$，$t\not\sqsubset term(\langle s,j\rangle)$，则称项 t 源发于结点 n，若项 t 在串空间 Σ 中有且仅有一个源发结点 n，则称项 t 唯一源发于 n。

定义 3[3] 如果 $t\sqsubset n$ 且 t 为非级联项，同时所有满足 $t'\neq t$，且 $t\sqsubset t'\sqsubset n$ 的 t' 均为级联项，则称 t 是结点 n 的组件(component)。记 $n=\langle s,i\rangle$，若对任意的 $j<i$，有 t 不是 $\langle s,j\rangle$ 的组件，则称 t 是结点 n 的新组件。

定义 4[3] $t=\{h\}_K$，如果：(1)$a\sqsubset t$ 且 t 是 $n\in\Sigma$ 的组件；(2)t 不为任何常规结点 $n'\in\Sigma$ 的组件的真子项，则称 t 为 a 在 n 中的测试组件(test component)，同时 a 称为测试元。

定义 5[3] 在边 $n\Rightarrow^+n'$ 中，如果(n 为正，n' 为负)/(n 为负，n' 为正)，$a\sqsubset term(n)$，结点 n' 包含新组件 t'，并且 $a\sqsubset t'$，则称 $n\Rightarrow^+n'$ 为关于 a 的变换边(transformed edge)/变换进行边(transforming edge)。

引理 1[3](输出测试定理) 丛 C 中边 $n\Rightarrow^+n'$ 为 a 的变换边，$t=\{h\}_K$ 为 a 在 n 中的测试组件，如果 a 唯一源发于 n，且 $K^{-1}\notin P$，则有(1)存在常规结点 $m,m'\in C$ 使得 t 是 m 的组件并且 $m\Rightarrow^+m'$ 是 a 的变换进行边。(2)假设 a 仅出现在 m' 的组件 $t_1=\{h_1\}_{K_1}$ 中，并且 t_1 不是任何常规结点消息的组件的真子项，$K^{-1}\notin P$，则 C 中存在负的常规结点 m''，并且 t_1 为该结点的组件。

引理 2[3](输入测试定理) 丛 C 中边 $n\Rightarrow^+n'$ 为 a 的变换边，$t'=\{h\}_K$ 为 a 在 n' 中的测试组件，如果 a 唯一源发于 n，且 $K\notin P$，则存在常规结点 $m,m'\in C$ 使得 t' 是 m' 的组件并且 $m\Rightarrow^+m'$ 是 a 的变换进行边。

引理 3[3](主动测试定理) 丛 C 中负结点 $n\in C$，如果 a 唯一源发于 n，且 $t=\{h\}_K$ 为 a 在负结点 n 中的测试组件，$K\notin P$，则丛 C 中存在一个正常规结点 $m\in C$，t 是 m 的组件。

3 认证测试的局限性分析

由于认证测试是由 Guttman 等人在串空间模型的基础上提出来的，而串空间语义中仅有子项与组件这两个工具可以刻画消息项之间的结构关系，因此认证测试类的改进措施可以统一归结为 3 处：1)引入串空间模型中的子项来刻画存在于嵌套加密测试组件内部的认证结构；2)增加限制条件，防止认证主体在认证测试完成之前泄漏测试组件相关信息造成的认证失败；3)利用串空间模型中的子项与组件来刻画认证测试结论。但是仅利用串空间中的子项与组件这两个工具不

能灵活准确地描述复杂消息数据项之间的结构关系，从而不足以全面有效反映嵌套加密协议的复杂内部结构，造成认证测试类存在错误认证、实现上的冗余或认证不彻底等局限性。下面结合实例介绍认证测试类的上述局限性，并在实例中阐明我们引入等价类、类组件、安全加密元及安全包裹元等概念的必要性。

首先给出由于串空间语义不完善导致认证不彻底或认证错误的实例。

例 1　设丛 C 中存在如图 1 所示的消息序列，其中 N 唯一源发于 A，且 $K_S^{-1}, K_{AB} \notin P$。在一次协议实例化中，主体 A 作为发起者发送一个消息项 ABN，之后收到消息项 $\{ANK\}_{K_{AB}}$，$+ABN \Rightarrow -\{ANK\}_{K_{AB}}$ 为主体 A 的串的一条关于 N 的变换边。

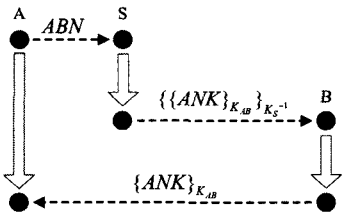

图 1　串空间语义缺乏导致的认证不彻底或认证错误

根据认证测试的测试原理，显然变换边 $+ABN \Rightarrow -\{ANK\}_{K_{AB}}$ 存在认证关系。且对于任意的认证测试类，该变换边仅可能关于 N 构成输入测试。由于串空间模型中仅有子项与组件这两个工具可以用于刻画消息项之间的结构关系，因此相应输入测试定理的结论仅可能为“C 中必然存在常规串结点 $m, m' \in C$，使得 $\{ANK\}_{K_{AB}}$ 是 m' 的组件/子项，且 $m \Rightarrow^+ m'$ 是 N 的变换进行边。”针对此结论，我们进一步分析：

若 $\{ANK\}_{K_{AB}}$ 是 m' 的组件[9-14]，对照图 1 所示的消息序列图，可得常规结点为主体 B 的串上的结点 $-\{\{ANK\}_{K_{AB}}\}_{K_S^{-1}}$ 及 $+\{ANK\}_{K_{AB}}$，这显然不符合实际情况。因为 K_S 攻击者可以公开获得，攻击者可以通过截获主体 S 发送的 $\{\{ANK\}_{K_{AB}}\}_{K_S^{-1}}$，生成 $\{ANK\}_{K_{AB}}$，直接发送给主体 A，而主体 B 却没有参与此次变换，这显然与认证结论相矛盾，从而导致错误的认证。

若 $\{ANK\}_{K_{AB}}$ 是 m' 的子项[7,8]，对照图 1 所示的消息序列图，可得无论是主体 B 的串，还是主体 S 的串都存在满足相应结论的变换边，其中 B 的串上变换边为 $-\{\{ANK\}_{K_{AB}}\}_{K_S^{-1}} \Rightarrow +\{ANK\}_{K_{AB}}$，$S$ 的串上变换边为 $-ABN \Rightarrow +\{\{ANK\}_{K_{AB}}\}_{K_S^{-1}}$。那么此时我们无法判断主体 B 和 S 的串的变换进行边上的结点都为常规结点，还是只有其中一个主体的串的变换进行边上的结点为常规结点；若为后者，也无法判断是主体 B 还是主体 S 的串上的变换进行边上的结点为常规节点，因而造成认证不彻底。

接着给出由于串空间语义不完善导致的实现上冗余的实例。

例 2　设丛 C 中存在如图 2 所示的消息序列，其中 N 唯一源发于 A，且 K_A^{-1}、K_B^{-1}、K_S^{-1}、$K_{AS} \notin P$。在一次协议实例化中，主体 A 作为发起者发送一个消息项 $\{\{\{AN\}_{K_B}\}_{K_{AS}}\}_{K_S^{-1}}$，经过若干次会话后收到消息项 $\{ANK_{AB}\}_{K_A}$。

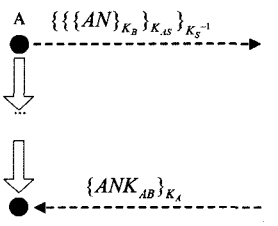

图 2　串空间语义缺乏导致的实现冗余

令 $n = +\{\{\{AN\}_{K_B}\}_{K_{AS}}\}_{K_S^{-1}}$，$n' = -\{ANK_{AB}\}_{K_A}$，则边 $n \Rightarrow n'$ 为主体 A 的串上的一条关于 N 的变换边。显然若攻击者不能直接从主体 A 所在串中任何 $<_C n'$ 的正结点 n'' 的消息项中通过自身能力（截获、加/解密、级联/拆分等）构造出 $\{ANK\}_{K_A}$，则变换边 $n \Rightarrow n'$ 存在认证关系。根据认证测试的测试原理，该变换边仅可能构成输出测试。相应的输出测试条件中测试边正串结点中包含测试元的加密结构也仅能选用“子项”或“组件”来刻画。针对此，我们进行以下分析：

若选用“组件”来刻画输出测试条件中测试边正串结点中包含测试元的加密结构，同样会造成认证不彻底的局限性。因此认证测试类中的大部分文献都选用“子项”来刻画输出测试条件中测试边正串结点中包含测试元的加密结构。且为了充分挖掘认证测试边所包含的所有认证测试信息，在应用输出测试定理进行认证测试分析时，需要对所有满足输出测试条件的加密子项都进行认证分析。但是，根据输出测试定理，对于同一个测试元，依靠测试边正串节点中任意包含该测试元的加密子项得出的认证结论是一样的。如例 2，对于测试元 N，依靠测试边 $+\{\{\{AN\}_{K_B}\}_{K_{AS}}\}_{K_S^{-1}} \Rightarrow^+ -\{ANK_{AB}\}_{K_A}$ 正串结点“$+\{\{\{AN\}_{K_B}\}_{K_{AS}}\}_{K_S^{-1}}$”中的加密子项 $\{AN\}_{K_B}$ 与 $\{\{AN\}_{K_B}\}_{K_{AS}}$ 得到的输出测试结论是一样的。因此，协议越复杂，测试组件嵌套加密层数越多，输出测试冗余越严重，极大地影响了实现的效率。

此外，串空间语义不完善还导致不易刻画认证测试的约束条件，该条件是为了防止认证主体在认证测试完成之前泄漏测试组件相关信息而造成认证失败。特别是对于输出测试定理，仅依靠组件与子项这两个工具很难给出一个形式化的约束条件，具体原因就不再举例介绍。

为解决上述局限性，本文通过在串空间模型中引入等价类、类组件、安全加密元及安全包裹元等概念，完善了串空间模型中有关刻画消息项之间及内部结构关系方面的语义，基于此提出了一种可以分析多层嵌套加密协议的优化认证测试方法，并从理论上给出了形式化证明，保证了新认证测试方法的正确性。

4　认证测试类的改进方案

首先对串空间模型中刻画消息项之间及内部结构关系的语义进行完善。引入等价类、类组件、安全加密元及安全包裹元等概念。

定义 6　设 g 与 h_i 为丛结点的任意项，$0 \leqslant i \leqslant n$，称形如 gh_1 或者 $\{\{\{gh_1\}_{k_1} h_2\}_{k_2} \cdots\}_{k_{n-1}} h_n\}_{k_n}$ 的消息项为 g 的等价类，记为 Γ_g，其中 $n \geqslant 1$，$1 \leqslant i \leqslant n$，$k_i^{-1} \in P$，$h_i$ 为可选项（即可有可无）。

由定义 6，攻击者只要获得某消息项的任一等价类，就可以利用自己的能力得到该消息项。

定义 7 设 m 为丛 C 的一个结点，攻击者仅利用解密操作对 m 解密得到的新消息项为 m'，则称 m' 的组件为消息项 m 的类组件。

例如，令 $m=\{\{AKN_A\}_{K_{AB}}\}_{K_A^{-1}}N_B\}_{K_S^{-1}}$，其中 $K_A,K_S\in P,K_{AB}\notin P$，则 $m=\{\{AKN_A\}_{K_{AB}}\}_{K_A^{-1}}N_B\}_{K_S^{-1}}$ 的类组件为 $\{AKN_A\}_{K_{AB}}$ 与 N_B。

由定义 7 可知，若攻击者可以获得某一消息项，则攻击者可以利用自己的能力直接获得该消息项的所有类组件。因而消息项的安全性完全由其类组件的安全性决定。

定义 8 设 t 为丛 C 中结点 m 的组件，$h_0\subset t$，若 $t'=\{h\}_K\subset t,h_0\subset t'$，且 $K\notin P$，则称 t' 为 h_0 关于组件 t 的安全加密元。若组件 t 中不存在以 t' 为真子项的 h_0 的安全加密元，则称 t' 为 h_0 关于组件 t 的最大安全加密元。

定义 9 设 t 为丛 C 中结点 m 的组件，$h_0\subset t$，若 $t'=\{h\}_K\subset t,h_0\subset t'$，且 $K^{-1}\notin P$，则称 t' 为 h_0 关于组件 t 的安全包裹元。若组件 t 中不存在以 t' 为真子项的 h_0 的安全包裹元，则称 t' 为 h_0 关于组件 t 的最大安全包裹元。若 h_0 关于组件 t 的安全包裹元 $t'=\{\{\{(m_1h_0\}_{k_1}m_2\}_{k_2}\cdots\}_{k_{n-1}}m_n\}_{k_n}$，其中 $n\geqslant 1,1\leqslant i\leqslant n,k_i^{-1}\notin P,m_i$ 为可选项，且 $h_0\not\subset m_i$，则称 t' 为 h_0 关于组件 t 的强安全包裹元。

下面基于扩展后的串空间语义，给出新的认证测试方法，称之为强认证测试。其由 3 个测试定理组成。

定理 1(强输入测试定理) 设丛 C 中存在边 $n\Rightarrow^+n'$，消息项 a 唯一源发于 n，t' 为 n' 的组件，如果存在加密子项 $t=\{h\}_K$ 满足 $a\subset t\subset t'$，并且 n 所在串 s 中所有满足 $n''\prec_C n'$ 的正结点 n'' 都有 $t\not\subset term(n'')$，$K\notin P$，则丛 C 中一定存在常规串结点 m、m'，及 t 的某个关于 t' 的强安全包裹元 t_1，使得 t_1 的某个攻击等价类元是 a 关于组件 t' 的最大安全加密元，并且边 $m\Rightarrow^+m'$ 是 a 的变换进行边。

证明：若加密子项 $t=\{h\}_K$ 满足 $a\subset t\subset t',K\notin P$ 时，t_2 为 t 关于 t' 的任意强安全包裹元的任意攻击等价类元，且 t_2 为 a 关于组件 t' 的最大安全加密元。设 Ψ 为丛 C 中所有以 t_2 为子项的串结点构成的集合。由于 $t\subset t_2$，故 Ψ 中任意元素 n_i 都满足 $t\subset term(n_i)$。因为 $n'\in\Psi$，所以集合 Ψ 非空。又因为丛中任何非空串结点集均存在 $\prec_C$-*minimal* 元，所以可知集合 Ψ 存在 $\prec_C$-*minimal* 元，记为 m'。由于 S 中满足 $n''\prec_C n'$ 的所有结点 n'' 都有 $t\not\subset term(n'')$，则 S 中所有 $\prec_C n'$ 的结点都不在集合 Ψ 中，故 $n\neq m'$。由于 a 唯一源发于 n，且 $n\neq m'$，因此 a 不能源发于 m'。同时根据 $\prec_C$-*minimal* 元的定义，m' 为正，故 m' 所在串上至少存在一个结点 m_0 满足 $m_0\Rightarrow^+m'$ 并且 $a\subset term(m_0)$，令 m 是满足 $m_0\Rightarrow^+m'$ 并且 $a\subset term(m_0)$ 的 m_0 中最小的结点。

假设 $m=n$，则 Ψ 的最小元素 m' 位于串 S 上，由于 S 中所有 $\prec n'$ 的正结点 n'' 都有 $t\not\subset term(n'')$，故 m' 只可能为 n'。但是由于 n' 为负结点，而 m' 为正，故假设不成立。因此，$m\neq n$，即 a 同样不能源发于 m，则 m 为负。由于 m' 为 Ψ 中的 $\prec_C$-*minimal* 元素，故 $m\notin\Psi$，则有 $t\not\subset m$。根据变换进行边的定义，m 为负，m' 为正，$a\subset term(m)$，结点 m' 中包含新元素 t，并且 $a\subset t$，故 $m\Rightarrow^+m'$ 是 a 的变换进行边。下证边 $m\Rightarrow^+m'$ 一定在常规串上。

假设变换进行边 $m\Rightarrow^+m'$ 不在常规串上，由于 m' 出现了新组件，$m\Rightarrow^+m'$ 只能位于 D-串或者 E-串上。假设 $m\Rightarrow^+m'$ 位于 D-串，则 $term(m)$ 形如 $\{h'\}_{K'}$，显然 $t\subset h'=\{h'\}_{K'},t\subset term(m)$。而这与 m' 是集合 Ψ 的最小元素相矛盾，因此，$m\Rightarrow^+m'$ 不可能位于 D-串上。假设 $m\Rightarrow^+m'$ 位于 E-串，则 $term(m')$ 应形为 $\{h'\}_{K'}$，由于 $K\notin P,K'\neq K$，因此有 $t\subset h',t\subset term(m)$，与 m' 是集合 Ψ 的最小元素相矛盾，故 $m\Rightarrow^+m'$ 不可能位于 E-串上。即 m 与 m' 为常规结点，且丛 C 中存在 t 的某个关于 t' 的强安全包裹元 t_1，使得 t_1 的某个攻击等价类元是 a 关于组件 t' 的最大安全加密元，并且边 $m\Rightarrow^+m'$ 是 a 的变换进行边。

接着算法 1 给出了强输入测试定理测试边负串结点加密子项的选取规则，既消除了强输入测试定理的认证冗余，又能遍历测试边负串结点中关于同一个测试元存在认证信息的所有加密子项。

算法 1 强输入测试加密子项选取算法

Step 1 令 t 为 a 关于 t'的最大安全加密元。

Step 2 判断 t 是否满足强输入测试定理的条件，若不满足，终止；否则，输出相应的认证测试结论。

Step 3 判断是否存在结点 $n_1\leqslant_C m'$，且 n_1 不在 s 串上，使 n_1 的某个加密子项为 t 真子项的某个关于 t'的强安全包裹元的等价类。若存在，则 t 更新为满足该条件最大的 n_1 结点所对应的 t 的真子项，且转至 Step 2；否则，终止。

由算法 1 显然可知，若通过其选取的每个加密子项满足强输入测试定理的条件，则由其推出的常规串结点都不相同，即输出不同的认证测试结论，从而消除了强输入测试定理的认证冗余。同时由于算法 1 是按照回溯法，先找到丛 C 中离 n' 最近的常规结点，即当 t 为 a 关于 t' 的最大安全加密元时确定的常规结点，再以此常规结点为基点，确定离该常规串结点最近的常规串结点，依次类推，因此我们的选取规则遍历了测试边负串结点中关于同一个测试元 a 存在认证信息的所有加密子项。并且协议越复杂，测试组件嵌套加密层数越多，强输入测试定理的认证分析效率越高。

定理 2(强输出测试定理) 设丛 C 中存在边 $n\Rightarrow^+n'$，消息项 a 唯一源发于 n，t 为 n 的组件，t_0 为 t 关于 a 的最大安全包裹元。如果 $t_0\not\subset term(n')$，且 $a\subset term(n')$，对于 n 所在串 s 中 $\prec_C n'$ 的任意正串结点，其任何包含消息项 a 的类组件 t' 都满足 $t_0\subset t'$。则

(1)C 中存在常规结点 $m,m'\in C$，使得 $t_0\subset m$，且 $m\Rightarrow^+m'$ 是 a 的变换进行边。

(2)将 m,m' 所在主体串记为 s'，假设 a 仅出现在结点 m' 的组件 $t_1=\{h_1\}_{K_1}$ 中，并且串 s' 的所有正结点中不以除 t_1 以外的形式出现，$K_1^{-1}\notin P$，则 C 中存在负的常规结点，使得 t_1 为该结点的子项。

证明：(1)构造集合 Ψ，令 $\Psi=\{n_0\mid a\subset term(n_0)$ 且 $t_0\not\subset term(n_i)\}$。由于 $n'\in\Psi$，因此 Ψ 非空。丛中结点的任何非空子集均有 $\prec_C$-*minimal* 元素，因此集合 Ψ 存在 $\prec_C$ 上的最小元素，记为 m'，且 m' 为正。由于 $n\notin\Psi,n\neq m'$，且 a 唯一源发于 n，则 a 不能源发于 m'，故 m' 所在串上至少存在一个结点 m_0 满足 $m_0\Rightarrow^+m'$ 并且 $a\subset term(m_0)$，令 m 是上述 m_0 中最小的结点。假设 $m=n$，则集合 Ψ 的最小元素 m' 也位于串 s 上，而 s 的所有 $\prec_C n'$ 的正结点 n'' 中，若其任何类组件 t' 满足 $a\subset t'$，则必然有 $t_0\subset t'$，故 m' 只可能为 n'。但 n' 为负结点，而 m' 为正，故假设不成立。因此，$m\neq n,a$ 同样不能源发于 m，由此可得 m 为负。由于 m' 为 Ψ 中的 $\prec_C$-*minimal* 元素，故 $m\notin\Psi$，又因为 $a\subset term(m)$，所以 $t_0\subset term(m)$。根据变换进行边的

定义，m 为负，m' 为正，$a \sqsubset term(m)$，结点 m' 中包含新组件 t_1 并且 $a \sqsubset t_1$，因此 $m \Rightarrow^+ m'$ 即为 a 的变换进行边。下证边 $m \Rightarrow^+ m'$ 一定在常规串上。

如果变换进行边 $m \Rightarrow^+ m'$ 不在常规串上，则 $m \Rightarrow^+ m'$ 只可能位于 D-串或者 E-串。如果 $m \Rightarrow^+ m'$ 位于 D-串，由于 $K^{-1} \notin P$，D-串的密钥边不可能是 K^{-1}，故 $term(m)$ 形如 $\{h'\}_{K'}$，其中 $K' \neq K$，$t_0 \sqsubset term(m) = \{h'\}_{K'}$，因此 $t_0 \sqsubset h = term(m')$。而这与是集合 Ψ 最小元素相矛盾，因此 $n_0' \Rightarrow^+ n_0$ 不可能位于 D-串上。如果 $m \Rightarrow^+ m'$ 位于 E-串，$term(m')$ 应形为 $\{h'\}_{K'}$，显然 $t_0 \sqsubset term(m) = h'$，亦有 $t_0 \sqsubset \{h'\}_{K'} \sqsubset term(m')$，与 $m \in \Psi$ 矛盾，因此 $m \Rightarrow^+ m'$ 也不可能位于 E-串。故变换进行边 $m \Rightarrow^+ m'$ 只可能位于常规串上。

故 C 中必然存在常规结点 $m, m' \in C$，使得 $t_0 \sqsubset m$，并且 $m \Rightarrow^+ m'$ 是 a 的变换进行边。

(2)令 n' 中包含 a 的新组件为 t'，如果 $t' = t_1$，那么显然存在负的常规结点 n'，使得 t_1 为该结点的子项。

若 $t_1 \neq t'$，则构造集合 Ψ'，使得集合中的任意元素 n_0' 满足 $\succ_C n_0'$，$a \sqsubset n_0'$，并且 $t_1 \not\sqsubset term(n_0')$。由于 $n' \in \Psi'$，因此 Ψ' 非空。丛中任何非空子集均存在最小元，则集合 Ψ' 存在 $\prec_C$ 上的最小元，记为 u'，由最小元的性质知 u' 为正。又因为 $u' \succ_C m'$，m' 也为正结点，则丛 C 中必然存在一负的结点 $u_0' \Rightarrow u'$，且 $u_0' \succ_C m'$，$a \sqsubset u_0'$，因此 $t_1 \sqsubset term(u_0')$。下证负串结点 u_0' 一定为常规串结点。

根据变换进行边的定义，易知 $u_0' \Rightarrow^+ u'$ 构成 a 的变换进行边。假设 $u_0' \Rightarrow^+ u'$ 不在常规串上，由于 u' 出现了新组件，$u_0' \Rightarrow^+ u'$ 只能位于 D-串或者 E-串中。假设 $u_0' \Rightarrow^+ u'$ 位于 D-串，由于 $K_1^{-1} \notin P$，D-串的密钥边不可能是 K_1^{-1}，故 $term(u_0')$ 形如 $\{h'\}_{K'}$，其中 $K' \neq K_1$，则有 $t_1 \sqsubset h' = u'$，与 $u' \sqsubset \Psi'$ 相矛盾，因此，$u_0' \Rightarrow^+ u'$ 不在 D-串上。假设 $u_0' \Rightarrow^+ u'$ 位于 E-串，则 $t_1 \sqsubset term(u_0') \sqsubset term(u')$，与 $u' \sqsubset \Psi'$ 相矛盾，因此，$u_0' \Rightarrow^+ u'$ 不在 E-串上。则 $u_0' \Rightarrow^+ u'$ 位于常规串上，即负串结点一定为常规串结点。

故 C 中必然存在负的常规结点，t_1 为该结点的子项。

定理 3(强主动测试定理) 设 n 为丛 C 的一个负结点，t 为 n 的组件，如果存在加密子项 $t' = \{h\}_K$ 满足 $a \sqsubset t' \sqsubset t$，并且对于 n 所在串 s 中所有满足 $n' \prec_C n$ 的正结点 n' 都有 $t' \not\sqsubset term(n')$，则丛 C 中一定存在常规串结点 m，及 t 的某个关于 t' 的强安全包裹元 t_1，使得 t_1 的某个攻击等价类元是 a 关于组件 t 的最大安全加密元。

证明过程类似定理 1，在此省略。同样为了消除强主动测试认证冗余，同时又能遍历关于同一个测试元存在认证信息的所有加密子项，强主动测试定理负串结点的加密子项可按算法 1 进行选取。

接着算法 1 给出了强输入测试定理测试边负串结点加密子项的选取规则，既消除了强输入测试定理的认证冗余，又能遍历测试边负串结点中关于同一个测试元存在认证信息的所有加密子项。

综上，本文提出的强认证测试很好地解决了认证测试在多层嵌套加密协议分析时存在的错误认证、实现上冗余及认证不彻底等局限性。并且协议越复杂，测试组件嵌套加密层数越多，强认证测试的认证分析效率越高。下面将使用强认证测试，以 SPLICE/AS 协议[15]为例阐述强认证测试的应用过程。

例 3 SPLICE/AS 协议是一个关于客户和服务器进行双向认证的协议，认证过程中使用了一个证书授权机构 AS 来分配密钥。该协议消息序列如图 3 所示。

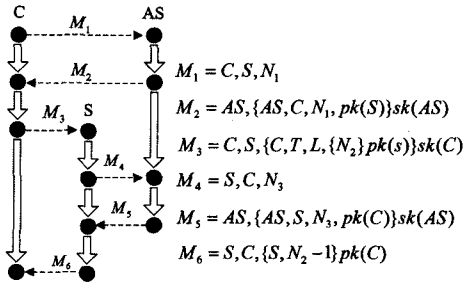

图 3 SPLICE/AS 协议的消息图

SPLICE/AS 协议串空间 Σ，包括以下 4 类串集合：

(1)发起者串 $init[C, S, AS, N_1, N_2, T, L, H = K_{S'}]$ 的消息迹为

$\langle + CSN_1, - AS\{ASCN_1\ K_{S'}\}_{K_{AS}^{-1}}, + CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}, -SC\{S(N_2 - 1)\}_{K_C} \rangle$

(2)响应者串 $resp[C, S, AS, N_2, N_3, T, L, H = K_{S'}, H' = K_{C'}]$ 的消息迹为

$\langle -CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}, +SCN_3, -AS\{ASSN_3 K_{C'}\}_{K_{AS}^{-1}}, +SC\{SN\}_{K_{C'}} \rangle$

其中，$N = \{\{N_2\}_{K_{S'}}\}_{K_S^{-1}} - 1$。

(3)服务器串 $serv[C, S, AS, N_1, N_3, K_S, K_C]$ 的消息迹为 $\langle -CSN_1, +AS\{ASCN_1\ K_S\}_{K_{AS}^{-1}}, -SCN_3, +AS\{ASSN_3\ K_C\}_{K_{AS}^{-1}} \rangle$

(4)攻击者串 P

其中，H, H' 表示主体不能识别内容的公钥，分别用 $K_{S'}$、$K_{C'}$ 表示，T 表示时间戳，L 表示生命周期。

SPLICE/AS 协议有 3 个角色：发起者、响应者和服务器。协议的目的是发起者和响应者能够互相认证。下面用本节提出的强认证测试分别对发起者与响应者的认证情况进行分析，从而判定协议的认证目标是否达到。

(1)发起者的保证

定理 4 假设 C 为 Σ 上的一丛，$C \neq S, N_1, N_2$ 在 C 中唯一源发，并且 $K_{AS}^{-1}, K_C^{-1} \notin P$，$K_{AS}$ 可以通过 PKI 机制安全、可靠地公开获得。如果 $s \in init[C, S, AS, N_1, N_2, T, L, H]$ 在丛 C 中的高度 $C\text{-}height = 4$，则存在正常串 $s_{serv} \in Serv[C, S', AS, N_1, *, H = K_{S'}, K_C]$，且其在丛 C 中的高度 $C\text{-}height = 4$，$s_{resp} \in Resp[*, *, *, *, *, *, *, *, *, *]$ 且其在丛 C 中的高度 $C\text{-}height \geqslant 0$，其中 $*$ 表示发起者不能认证的内容。

证明：易证发起者串中 $+CSN_1 \Rightarrow^+ -AS\{ASCN_1\ H\}_{K_{AS}^{-1}}$ 关于 N_1 满足强输入测试定理，则 C 中必然存在常规结点 $m, m' \in C$，使得 $t = \{ASCN_1 H\}_{K_{AS}^{-1}}$ 的某个关于其自身的强安全包裹元等价类 $\Gamma_{t'}$ 为 t 关于 m' 某个以其为子项的组件的最大安全加密元，并且 $m \Rightarrow^+ m'$ 是 a 的变换进行边。观察协议消息格式，m, m' 分别只可能为服务器串的 $\langle s, 1 \rangle$，$\langle s, 2 \rangle$ 结点。故丛 C 中必然存在服务器串 $s_s \in serv[C, *, AS, N_1, *, K_{S'}, *]$，并且其 $C\text{-}height = 2$。

由 SPLICE/AS 协议机制知 K_C 只能源发于服务器串。由于发起者串的结点 $\langle s_i, 4 \rangle = -SC\{S(N_2 - 1)\}_{K_C}$，观察协议消息格式，$K_C$ 源发于服务器的结点 $\langle s, 4 \rangle$，则丛 C 中必然存在服务器串 $S_s \in serv[C, S', AS, N_1, *, K_{S'}, K_C]$，并且其

$C\text{-}height=4$。

攻击者可以发送信息 S,C,N' 给服务器，从而获得 K_C，其中 N' 为攻击者任意选取的随机数，则 $K_C\in P$，因此对照发起者的串消息形式，发起者串若存在其它认证测试，其只能是强输出测试，且只可能是 $+CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}\Rightarrow^{+}-SC\{S(N_2-1)\}_{K_C}$ 关于 N_2 构成强输出测试。判定其是否满足强输出测试的关键在于 $K_{S'}^{-1}$ 是否属于 P。若 $K_{S'}^{-1}\notin P$，则满足强输出测试定理，反之，则不满足。由于攻击者可以截获发起者发送的信息 C,S,N_1，并将其篡改为 C,P,N_1，发送给服务器，之后服务器将会发送信息 $AS\{ASCN_1K_P\}_{K_{AS}^{-1}}$ 给发起者，此时 $K_P^{-1}\in P$，即 $K_{S'}^{-1}$ 可能属于 P，因此 $+CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}\Rightarrow^{+}-SC\{S(N_2-1)\}_{K_C}$ 不满足强输出测试条件。综上认证结束，定理得证。

根据定理 4 的结论，我们发现发起者无法保证正常响应者 S 是否参与，同时虽然可以保证服务器 AS 全程参与，但发起者无法保证服务器是否是与正常的响应者 S 进行信息交换。因此 SPLICE/AS 协议可能存在以下两种攻击：(1)S 完全没有参与，攻击者利用发起者无法保证其是否与正常响应者进行信息交换，及服务器 AS 不知发起者要与哪个响应者进行信息交换的协议缺陷，冒充响应者进行攻击。(2)S 参与，攻击者利用响应者 S 不知道与哪个发起者进行信息交换，及服务器 AS 不知发起者要与哪个响应者进行信息交换的协议缺陷进行攻击。通过分析，我们认为上述两种攻击都是可行的。

下面分别给出具体攻击实例：对于第一种攻击，只需一次协议运行攻击者就可以成功扮演响应者，使 C 误以为已经与 S 建立连接，同时可以获取 N_2 的值，图 4 给出了相应的攻击实例。

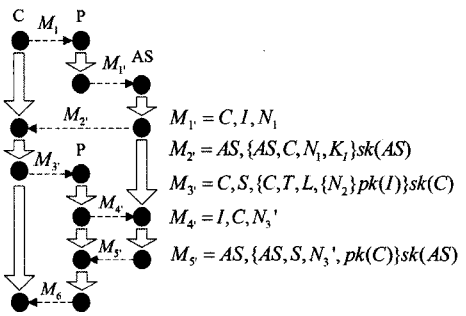

图 4　SPLICE/AS 协议攻击案例 1 的消息图

对于第二种攻击，攻击者只需要两次协议运行就可以成功使 C 误以为已经与 S 建立连接，而 S 却误以为是客户 I 申请与其建立连接。首先攻击者需要实例化一次协议来获得客户 C 的公钥 $pk(C)$，具体过程如图 5 所示。

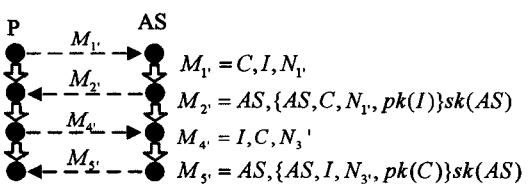

图 5　SPLICE/AS 协议中攻击者获取客户 C 公钥 $pk(C)$ 的攻击消息图

之后，攻击者在获得客户 C 的公钥 $pk(C)$ 的基础上，实施如图 6 所示的攻击。

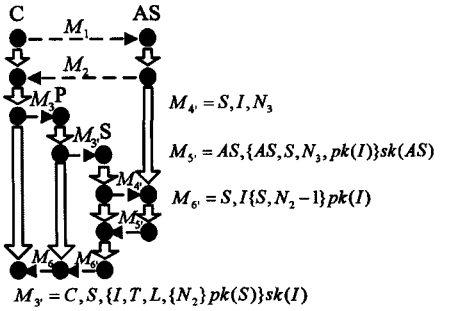

图 6　SPLICE/AS 协议攻击案例 2 的消息图

(2)响应者的保证

定理 5　假设 C 为 Σ 上的一丛，$S\neq C,N_3$ 在 C 中唯一源发，并且 $K_{AS^{-1}},K_{C^{-1}}\notin P,K_{AS}$ 可以通过 PKI 机制安全、可靠地公开获得。如果 $s\in resp[C,S,AS,N_2,N_3,T,L,H=K_{S'},H'=K_{C'}]$，且在丛 C 中的高度 $C\text{-}height=4$，则存在正常串 $s_{serv}\in serv[*,S,AS,*,N_3,K_S,*]$ 且其在丛 C 中的高度 $C\text{-}height=4$，$s_{init}\in init[*,*,*,*,*,*,*,*,*]$ 且其在丛 C 中的高度 $C\text{-}height\geqslant 0$。

证明：易证响应者串中 $+SCN_3\Rightarrow^{+}-AS\{ASSN_3K_{C'}\}_{K_{AS}^{-1}}$ 关于 N_3 满足强输入测试定理，则 C 中必然存在常规结点 $m,m'\in C$，使得 $t=\{ASSN_3K_{C'}\}_{K_{AS}^{-1}}$ 某个关于其自身的强安全包裹元的等价类 $\Gamma_{t'}$ 为 t 关于 m' 某个以其为子项的组件的最大安全加密元，并且 $m\Rightarrow^{+}m'$ 是 N_3 的变换进行边。观察协议消息格式，m,m' 分别只可能为服务器串的 $\langle s,3\rangle,\langle s,4\rangle$ 结点。故丛 C 中必然存在服务器串 $s_s\in serv[*,S,AS,*,N_3,K_S,*]$，并且其 $C\text{-}height=4$。

对照发起者串消息形式，发起者串若存在其它认证测试，只能是强主动测试，且只可能是 $-CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}$。由前面证明知 $K_{S'}$ 可能属于 P，因此只有 $K_C^{-1}\notin P$ 时，$-CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}$ 满足强主动测试条件。但是由于攻击者可以截获发起者发送的信息 S,C,N_3，并将其篡改为 S,P,N_3，发送给服务器，之后服务器发送 $AS\{ASSN_3K_P\}_{K_{AS}^{-1}}$ 给 S，而 S 无法判定 K_P 是否为 C 的公钥，故 $\langle s_r,1\rangle$ 可能为 $-CS\{CTL\{N_2\}_{K_{S'}}\}_{K_P^{-1}}$，因此 K_C^{-1} 可能属于 P，所以 $-CS\{CTL\{N_2\}_{K_{S'}}\}_{K_C^{-1}}$ 不满足强主动测试条件。综上认证结束，定理得证。

根据定理 5 的结论，SPLICE/AS 协议还可能存在以下两种攻击：(1)C 完全没有参与，攻击者利用响应者无法保证其是否与正常发起者 C 进行信息交换，及服务器 AS 不知响应者要与哪个发起者进行信息交换的协议缺陷，冒充发起者进行攻击；(2)C 参与，由于发起者知道要与哪个响应者 S 进行信息交换，这点攻击者没法欺骗发起者。攻击者唯一能利用的协议缺陷就是服务器 AS 不知哪个发起者要与响应者 S 进行信息交换来进行攻击。

通过分析，我们发现第一种攻击是成功可行的，具体过程如图 7 所示。

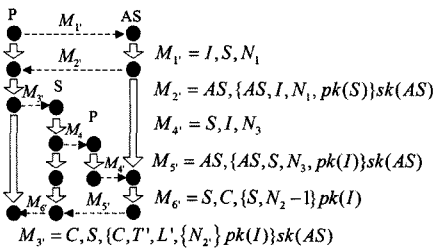

图 7　SPLICE/AS 协议攻击实例 3 的消息图

(下转第 169 页)

密数据识别方案相比，本文提出的方案适用性更好、识别率更高。

参 考 文 献

[1] 龙文，马坤，辛阳，等. 适用于协议特征提取的关联规则改进算法[J]. 电子科技大学学报，2010，39(2)：302-305

[2] Charles V W，Fabian M，Gerald M M. On inferring application protocol behaviors in encrypted network traffic[J]. Journal of Machine Learning Research，2006，7(12)：2745-2769

[3] Sun Guang-lu，Xue Yi-bo，Dong Ying-fei，et al. A Novel Hybrid Method for Effectively Classifying Encrypted Traffic[C]// Proceedings of Communications and Systems Security，2010，GLOBECOM 2010. Miami USA，2010 IEEE，2010：1-5

[4] Talieh S T，Mostafa A，Fakhri K，et al. Machine Learning-Based Classification of Encrypted Internet Traffic[C]// 8th International Conference，MLDM 2012. Berlin，Germany，2012：578-592

[5] Zhang Meng，Zhang Hong-li，Zhang Bo. Encrypted Traffic Classification Based on an Improved Clustering Algorithm[C]// International Conference，ISCTCS 2012. Beijing，China，2012：124-131

[6] Du Ye，Zhang Ru-hui. Design of a method for encrypted P2P traffic identification using K-means algorithm [J]. Telecommunication Systems，2013，53(1)：163-168

[7] 赵博，郭虹，刘勤让，等. 基于加权累积和检验的加密流量盲识别算法[J]. 软件学报，2013，24(6)：1334-1345

[8] Menezes A J，Van O P C，Vanstone S A. 应用密码学手册 [M]. 胡磊，王鹏，等译. 北京：电子工业出版社，2005：1-4

[9] NIST FIPS PUB 140-2-2001. Security Requirements for Cryptographic Modules[S]. Washington DC，USA：National Institute of Standards and Technology，2001

[10] NIST SP800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications Revision 1a[S]. Washington DC，USA：National Institute of Standards and Technology，2010

[11] 徐晶，于向军. 基于 FFT 算法的震动信号分析[J]. 工业控制计算机，2005，18(12)：8-9

(上接第 154 页)

在上面的实例中，只需一次协议运行，攻击者就可以成功扮演发起者 C，使 S 误以为客户 C 已经与自己建立连接。

第二种攻击中所提出的安全漏洞，可能会威胁协议的安全性，但我们还未能给出攻击实例。

扮演其它角色的正常主体参与此次协议会话主要取决于其对应的串在丛中的高度与串参数值这两个因素。对于任何角色串，通过我们的强认证测试可以很容易地确定出其它合法主体串的这两个因素值。前者决定扮演协议的其它诚实主体参与此次协议变换的步数，后者决定该诚实主体进行交互消息项的具体值。进而就可以清晰地判断出协议中该角色的认证目标是否可以达到。同时还可通过强认证测试最终确定出其它合法主体串的参数值中不能认证的参数，来指导协议攻击实例的构造。

结束语 本文分析了认证测试类在分析多层嵌套加密协议的局限性，扩展了串空间理论刻画消息项之间及内部结构关系的能力。在此基础上，提出了一种可以分析协议测试组件嵌套加密的通用的认证测试优化方案，并使用串空间理论对其进行了形式化证明，同时通过具体协议实例验证了强认证测试方法在应用范围上的突破及有效性。由于目前认证测试方法在类型缺陷分析方面存在较大局限性，能否进一步改进强认证测试方法，使其能够分析协议类型缺陷攻击，还值得进一步研究[16]。

参 考 文 献

[1] Fabrega F J T，Herzog J C，Guttman J D. Strand space：Why is a security protocol correct[C]// IEEE Computer Society Press Proc. of the IEEE Symp. on Research in Security and Privacy. Oakland，1998：160-171

[2] Meadows C. Open issues in formal methods for cryptographic protocol analysis[C]// Proceedings，IEEE DARPA Information Survivability Conference and Exposition. 2000，1：237-250

[3] Guttman J D，Thayer F J. Authentication tests [C]// Proceedings，2000 IEEE Symposium on Security and Privacy. IEEE Computer Society Press，May 2000：96-109

[4] Guttman J D. Security protocol design via authentication tests [C]// Proceedings Computer Security Foundations Workshop，2002. 15th IEEE. IEEE，2002：92-103

[5] Wang Q，Zhi F H，Ao J H. Design and Security Analysis of Mobile Identity Authentication Protocol[J]. Advanced Materials Research，2012，403：2645-2649

[6] Chen N，Jiang R. Security Analysis and Improvement of User Authentication Framework for Cloud Computing[J]. Journal of Networks，2014，9(1)：198-203

[7] Perrig A，Song D. Looking for diamonds in the desert-extending automatic protocol generation to three-party authentication and key agreement[C]// Proc. of the 13th Computer Security Foundations Workshop. Los Alamitos：IEEE Computer Society Press，2000：64-76

[8] Li Y J，Pang J. Generalized unsolicited tests for authentication protocol analysis[C]// IEEE Computer Society Press Proc. of the 7th Int'l Conf. on Parallel and Distributed Computing，Applications and Technologies. 2006：509-514

[9] Liu J F，Zhou M T. Research and improvement on authentication test's limitation[J]. High Technology Letters，2008，14(3)：266-270

[10] 刘家芬，周明天. 突破认证测试方法的局限性[J]. 软件学报，2009，20(10)：2799-2809

[11] Zhang G，Rong M，Fang Y. One extension of authentication test based on strand space model[C]// Proc. of the 5th International Conference on Wireless Communications，Networking and Mobile Computing. IEEE Press，2009：4506-4509

[12] Zhou Q，Wu X. Extensions to Authentication Test and Its Application[J]. Journal of Zhengzhou University (Engineering Science)，2010，3：014

[13] Wang Q，Zhi F H，Ao J H. Design and Security Analysis of Mobile Identity Authentication Protocol[J]. Advanced Materials Research，2012，403：2645-2649

[14] Muhammad S. Applying authentication tests to discover Man-In-The-Middle attack in security protocols[C]// Eighth International Conference on Digital Information Management (ICDIM)，2013. IEEE，2013：35-40

[15] 余磊，魏仕民. 协议主体密钥在测试组件构造上的性质分析[J]. 计算机工程与应用，2013，49(6)：114-117

[16] Khot R A，Srinathan K，Kumaraguru P. A novel Jigsaw based authentication scheme using tagging[C]// Proc. of the 2011 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011：2605-2614