基于串空间认证测试理论的认证协议分析*

翁艳琴[1,2],石曙东[2],解颜铭[1,2]

(1.湖北师范学院 数学与统计学院,湖北 黄石 435000;
2.湖北师范学院 计算机科学与技术学院,湖北 黄石 435000)

摘 要:对增强型认证测试理论进行简化,使其能更好、更高效地分析协议的认证性。将其应用到对 OR 协议的分析中,发现协议存在的缺陷,对协议进行改进,并对改进后的协议进行了分析验证。

关键词:串空间模型;认证测试;关联性理论

中图分类号:TP309 **文献标识码**:A **文章编号**:1674-7720(2012)01-0051-04

Authentication protocol analysis based on certification test theory in strand space

Weng Yanqin[1,2], Shi Shudong[2], Xie Yanming[1,2]

(1.Institute of Mathematics and Statistical, Hubei Normal University, Huangshi 435000, China;
2.Institute of Computer Science and Technology, Hubei Nomal University, Huangshi 435000, China)

Abstract: This paper simplifies the theory of enhanced certification testing to make it better for analysis of authentication protocols, and by applicating it to the analysis of the OR agreement, it finds defects in agreement. The agreement is modified, and the improved authentication protocol is also verified.

Key words: strand space theory; certification testing; relevance concepts

串空间模型[1-2]是由 THAYER、HERZOG 和 GUTTMAN 三人于 1998 年提出来的,它吸纳了 NRL 协议器、Schneider 秩函数和 Paulson 归纳法等方法的思想,将协议的描述和目标安全属性转化为图结构,借助图的理论和算法进行协议安全性分析。认证测试[4-5]理论是在串(Strand)空间模型的基础上发展而来的一种基于挑战-响应概念的协议分析技术。AT 概念提供了简洁、强大的协议分析能力,它对协议不正确的判断基于 Strand 参数的不一致性,可用于协议的分析和设计。增强型认证测试理论是在串空间模型的基础上,借助认证测试理论,运用 AT 中协议判断分析的思想,通过由果导因的推理模式分析协议的关联性进而对协议的认证性进行验证。

本文对增强型认证测试理论进行简化,使得它对协议的认证性分析更加简洁、高效,将其应用到协议的安全性分析中,同时提出对协议认证性分析的一般模式,并将其应用到对 OR 协议的分析中,发现协议存在的漏洞,对 OR 协议进行了改进,并对改进后的协议进行了验证。

1 串空间内认证测试理论

串空间内认证测试理论的基本思想是,如果协议的一个主体发送了包含某个特定值 a (明文或者密文形式)的消息,并在之后收到改变了形式后的 a 值(被加密或者解密),那么可以肯定存在一个持有相应密钥的普通协议主体参与了该协议的执行。本文涉及的相关定义和概念如下:

定义 1(Component) 项 t0 是 t 的组件⇔

当且仅当 t、t0 不属于级联类型,并且对于任意 t1≠t0,如果有 t0⊂t1⊂t,那么,t1 属于级联类型。消息组件则是原子数据类型或者加密类型。

定义 2 (Transformed Edge 和 Transforming Edge)设 a∈A,n1 和 n2 为同一串中的节点,则:边 n1⇒+n2 是关于值 a 的被转换边⇔当且仅当 a 在节点 n1 发送,并在节点 n2 从新组件中接收。边是 n1⇒+n2 关于值 a 的转

*基金项目:湖北省自然科学基金(2006ABA056);湖北省教育厅重点项目(D20092203);湖北省教育厅青年项目(Q20102503)

换边⇔当且仅当 a 在节点 n1 接收，并在节点 n2 存在于新组件中发送。

定义 3 (Test Component 和 Test) t={h}k 是节点 n 关于 a 的测试组件⇔

①a⊂t，并且 t 是节点 n 的组件；

②t 不是串空间中任意其他正常节点的组件的子项。

边 n1⇒⁺n2 是 a 的一个测试⇔

如果值 a 在节点 n1 唯一生成，并且边 n1⇒⁺n2 是关于 a 的 Transformed Edge。

对应于挑战方-响应方对值 a 不同的加解密处理，参考文献 [4] 将认证测试划分为 Incoming Test (IT)、Outgoing Test (OT) 和 Unsolicited Test (UT) 3 种类型。其中，OT 和 IT 测试在增强型认证测试理论中可以进行简化，主要有以下两项：

方法 1 (OT)

边 n1⇒⁺n2 是项 t ={h}k 关于值 a 的输出认证测试 (OT)，如果：

①边 n1⇒⁺n2 是 a 的一个测试；

②$k^{-1} \notin Kp$；

③a 不在节点 n1 的除 t 以外的任何其他组件中出现；

④t 是节点 n1 关于 a 的一个测试组件。

方法 2 (UT)

接收节点 (负节点) n 是项 t={h}k 关于值 a 的主动认证测试 (UT)，如果：

①t 是节点 n 关于 a 的一个测试组件；

②$k \notin Kp$。

2 AT 中 Strand 参数一致性判断定理

参考文献[3]认为 Strand 参数可以分为 Nonce 参数、协商数据和主体标志 3 类，在主体 A 发起的与主体 S 之间的认证测试过程中，只有同时满足三类一致性才满足 Strand 参数的一致性。

(1) A 能确定在 Nonce 类型参数上与 S 的一致性；

(2) 当且仅当认证测试的数据满足表 1 中的要求，A 能确定与 S 在主体标志参数上的一致性；

(3) 当且仅当协商数据包含在测试组件中，A 能确定协商数据满足一致性。

表 1 给出了 A 发起与 S 的认证测试时，在不同加密方式下，各 Strand 的参数在某主体标志 X 上要达到一致所需满足的条件。

其中符号的含义如下：

id (A, X, S)：主体标志，包含 id (A, A, S) 和 id (A, B, S)。在协议 Strand 空间 $\sum$ 中，id (A, A, S) 表示主体 A 确定原子数据 t∈A 是 A 对于主体 S 的身份标志，即 A 可以确认的 A 相对 S 的身份标志，则必须有 t=A 或者 $t=Ka^{-1} \wedge t \notin P$ 或者 t=Kas∧t∉P 或者 t 是 A 与 S 之间共享的秘密才可以满足。而 id (A, B, S) 表示 Strand 空间 $\sum$ 中主体 A 确定原子数据 t∈A 是 B 对于主体 S 的身份标志，即 A 可以确认的 B 相对 S 的身份标志，则必须有 t=B 或者 t 是 A 能够确认被 S 所知的 A 与 B 之间共享秘密才可满足。C 表示主体标志必须包含在挑战 (Challenge) 内；R 表示必须包含在响应 (Response) 内；× 表示不满足认证测试要求；OK 表示在 A 与 S 交互中，id (A, A, S) 就是作为主体 A 能确认的 A 相对 S 的标志。表 1 列中不带方括号的内容给出的是在 A 与 S 两方进行交互的过程中的主体标志的参数一致性要满足的条件；带方括号表示 A、S、B 三方交互时主体标志的参数一致性需要附加的条件。

表 1 Strand 参数一致性

A			测试类型	S 响应类型 1 NULL	2 Kas	3 Ka^{-1}	4 Ka	5 Ks^{-1}	6 Ks
挑战加密类型	1	NULL	UT	×	OK[R]	×	×	R	×
	2	Kas	OT	OK[C]	OK[C/R]	×	OK[C/R]	OK[C/R]	×
	3	Ka^{-1}	UT	×	OK[C/R]	×	×	R	×
	4	Ka	×	×	×	×	×	×	×
	5	Ks^{-1}	×	×	×	×	×	×	×
	6	Ks	OT	C	OK[C/R]	×	C	C/R	×

3 增强型认证测试理论

针对认证测试理论中的认证测试方法，结合 Strand 参数一致性定理和关联规则，给出增强型认证测试的两种规则。

(1) 规则 1

假设 C 是某协议 Strand 空间的线束，节点 n2∈C，边 n1⇒⁺n2 是项 t 关于值 a 的 OT，则必然存在节点 m1、m2∈C 满足 t 是 m1 的消息组件，并且边 m1⇒⁺m2 是值 a 的 Transforming Edge；如果能满足 Strand 参数的一致性，那么对于 AT 的发起方来说，n1⇒⁺n2 和 m1⇒⁺m2 满足关联性。

(2) 规则 2

假设 C 是某协议 Strand 空间的线束，节点 n∈C，且 n 是项 t 关于值 a 的 UT，那么必然存在一个常规发送节点 m (正节点)∈C 满足 t 是 m 的消息组件；如果能满足 Strand 参数的一致性，那么对于 AT 的发起方来说，n 和 m 满足关联性。

4 关联度理论

定义 4：在 Strand 空间中，Corresp (AS) 表示协议主体 S 相对于 A 的关联度，Corresp (AS) ≥0。

Corresp (AS) 赋初值为 0，按 A 的 Strand 节点顺序依次考虑与 S 的认证测试 (OT，以及 S 向 A 提供的 UT)，

如果 S 的边<S,i>⇒<S,j>满足规则 n(n=1 或 2),则进行比较,如果 j>Corresp(AS),则 Corresp(AS)=j,否则 Corresp(AS)保持不变。用矩阵 M(A,S)可表示为:

M(A,S)=Corresp(AS),A=S

M(A,S)=Corresp(AS),A≠S

如果 Corresp(AS)=0,表示协议主体 A 不能确认与主体 S 的关联性;如果 Corresp(AS)=n>0,表示协议主体 A 能确认与主体 S 的 Strand 边<S,1>⇒⁺<S,n>的关联性。

5 增强型认证测试理论对协议的认证性分析

认证性对认证协议来说是其安全性的关键因素。增强型认证测试理论是一种针对协议的认证性进行分析的技术,它集合了基于 Strand 的认证测试理论、AT 中参数一致性理论以及关联性理论的优点,将协议分析规范化和模式化,抽象到数学矩阵的层次,为认证协议的分析提供了很好的工具。一般应用增强型认证测试理论对协议的认证性进行分析的步骤如下:

(1)将协议过程形式化,按照 Strand 理论的方法将各个主体之间联系起来构造 Strand 图;

(2)对协议中的参数按照 AT 中的 Nonce、协商数据和参与主体三种类型进行分类;

(3)按照主体的顺序依次分析每个主体与其他主体之间的关联性;

(4)将步骤(3)分析的结果构造成关联矩阵,分析判断协议的整体关联性;

(5)由协议的关联性分析判断协议的认证性是否满足要求,如果不满足则指明原因。

6 分析 OR 协议

OR 协议是一种有可信第三方参与的对称密钥协议,通过第三方 S 达成一致进行分配共享密钥 Kab。按照上面的步骤对 OR 协议进行分析,协议的过程如下:

(1)A→B:M,A,B,E(Kas:Na,M,A,B);

(2)B→S:M,A,B,E(Kas:Na,M,A,B),E(Kbs:Nb,M,A,B);

(3)S→B:M,E(Kas:Na,Kab),E(Kbs:Nb,Kab);

(4)B→A:M,E(Kas:Na,Kab)。

对应的 Strand 图如图 1 所示。

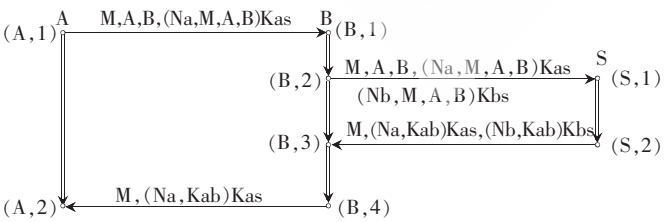

图 1 OR 协议的 Strand 图

对协议的参数分类如下:

Nonce 类型参数:Na,Nb;

协商数据参数:M,Kas,Kbs,Kab;

主体标志参数:A,B,S。

应用增强型认证测试理论对协议进行分析。

(1)对于协议的主体 A 进行分析。

由图 1 可看出,Na 是在 Strand 空间唯一生成的,term(A,1)={M,A,B,(Na,M,A,B)Kas},其中,(Na,M,A,B)Kas(Kas∉Kp)是(A,1)节点关于 Na 的测试组件。当其被 B 转发到 S 后,以新组件(Na,Kab)Kas 的形式在(A,2)节点接收,根据测试理论知:<A,1>⇒<A,2>是关于 Na 的输出认证测试,且由表 1 可知,只要满足 OK[C/R]就能满足主体标志一致性,即 A 与 S 协商过程中,主体 B 的标志应包含在相应组件中,而图 1 中 B⊂(Na,M,A,B)Kas 组件,故可以满足主体标志一致性。协商数 M,Kas⊂(Na,M,A,B)Kas,则在协商数 M、Kas 上也满足一致性,则由关联性规则 1 可得:<A,1>⇒<A,2>和<S,1>⇒<S,2>具有关联性,且有 Corresp(AS)=2。

(2)对主体 B 进行分析。

Nb 是在 Strand 空间唯一生成的,term(B,2)={M,A,B,(Na,M,A,B)Kas,(Nb,M,A,B)Kbs},其中,(Nb,M,A,B)Kbs(Kbs∉Kp)是(B,2)节点关于 Nb 的测试组件。根据测试理论可知:<B,2>⇒<B,3>是关于 Nb 的 OT,在 B 与 S 进行协商的过程由表 1 项可知,只要满足 OK 就能满足主体标志一致性,即主体为 B 和 S,由图知满足此条件,故满足主体标志一致性。协商数据 Kbs,M⊂(Nb,M,A,B)Kbs,则在协商数据 Kbs、M 上满足一致性。则由关联性规则 1 可得:<B,2>⇒<B,3>和<S,1>⇒<S,2>具有关联性,且有 Corresp(BS)=2。

(3)对于主体 S 进行分析。

在负节点(S,1)处,S 收到 term(B,2)={M,A,B,(Na,M,A,B)Kas,(Nb,M,A,B)Kbs},Na 和 Nb 是 Strand 空间唯一生成的,且 Kas,Kbs∉Kp,则(S,1)是关于 Na 和 Nb 的 UT。对于 Na 来自于 A,由表 1 知,符合主体标志一致性,结合关联度理论有 Corresp(SA)=1。同理,对 Nb 也满足主体标志一致性,结合关联度理论可得 Corresp(SB)=2。结合上面结果构造协议的关联矩阵如图 2 所示。

主体	A	B	S
A	2	0	2
B	0	4	2
S	1	2	2

图 2 OR 协议的关联矩阵

由图 2 可知:Corresp(AS)=2,A 能确认(S,1)⇒(S,2)的关联性;Corresp(BS)=2,B 能确认(S,1)⇒(S,2)的关联性;而 Corresp(AB)=0,Corresp(BA)=0,则 A 和 B 不能互相确认关联性。对协议整体来说,A,B 都可以确认与 S 的共识,但是不能确认 S 为其分配的共享密钥 Kab 在 A 和 B 之间进行交互时的确认,所以存在一定的安全隐患,可能导致信息的部分重放攻击。通过对 OR

协议的分析可看出增强型认证测试在对协议的认证性分析的有效性，还可以找出这个漏洞的原因来自于参数类型的不一致性。为了实现 A 和 B 之间的认证，针对此漏洞可以将协议作一些修改，修改后协议的 Strand 图如图 3 所示。

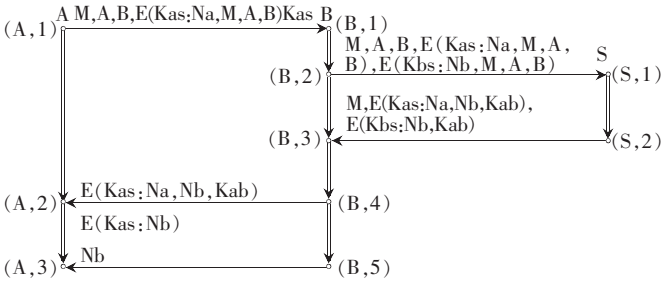

图 3 改进的 OR 协议的 Strand 图

协议中 A 和 B 之间通过 E(Kab:Nb)来实现认证性的关联，为了使得发起方 A 确认协商数是一致的，A 通过比较 Kas 加密的数据中的部分和 Kab 加密的数据来确认。可以用同样的方法对改进后的协议进行分析：(A,2)是关于 Nb 的 UT，Nb 来自于 B，由表 1 可得：A、B 满足主体参数一致性，在协商数 Kab 上也满足一致性，由关联规则 2 和关联度理论可得出 Corresp (AB)=4。<B,4>⇒<B,5>是关于 Nb 的 OT，由表 1 可知在 B 和 A 之间协商满足主体参数一致性，协商数据 Kab 也满足一致性，由关联规则 1 知<B,4>⇒<B,5>和<A,2>⇒<A,3>具有关联性，结合关联度定理有 Corresp(BA)=3。其他的关联度同原来的协议的分析相同。由此改进后的协议的关联矩阵如图 4 所示。

主体	A	B	S
A	3	4	2
B	3	5	2
S	1	2	2

图 4 改进的 OR 协议的关联矩阵

由图 4 可看出，Corresp(i j)≠0(i=A,B,S,j=A,B,S 且 i≠j)，故 A、B 和 S 三者之间可实现双向认证，具有认证性，在原协议的基础上进行了完善。

增强型认证测试理论从新的角度对协议进行了验证，推理过程简单，抽象到数学模型的层次，简单易用，为协议的形式化分析提供了新的思路。本文对增强型认证测试理论进行简化，将其应用到协议的安全性分析中，对 OR 协议进行了分析，发现存在的漏洞并有针对性地进行了改进，并对完善后的协议进行了验证。同时，本文还提出了协议认证性分析的一般模式，将协议分析规范化和模式化。本文提出的理论还存在许多需要完善的地方，如该方法目前只是在认证类协议中应用较多，对其他的协议还要推广扩充，对协议中并发问题的考虑等还需要相关研究者们的共同努力。

参考文献：

[1] Fàbrega F J T, HERZOG J C, GUTTMAN J D. Strand spaces: why is a security protocol correct?[C]. Proceedings of the 1998 IEEE Symposium on Security and Privacy, 1998:160-171.

[2] Fàbrega F J T, HERZOG J C, GUTTMAN J D. Strand spaces: proving security protocols correct [J]. Journal of Computer Security, 1999, 7(2-3):191-230.

[3] 杨明，罗军舟.基于认证测试的安全协议分析[J].软件学报，2006，17(01)：148-156.

[4] GUTTMAN J D, Fàbrega F J T. Authentication tests[C]. Proceedings of the 2000 IEEE Symposium on Security and Privacy, 2000:96-109.

[5] GUTTMAN J D, Fàbrega F J T. Authentication tests and the structure of bundles [J]. Theoretical Computer Science, 2002, 283(2):333-380.

[6] GUTTMAN J D. Security protocol design via authentication tests [C]. Proceedings of the 2002 IEEE Computer Security Foundations Workshop, 2002:92-103.

[7] WOO T Y C, LAM S S. A semantic model for authentication protocols [C]. Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy, 1993:178-194.

[8] Ji Q G, Qing S H, Zhou Y B, et al. Study on strand space model theory [J]. Journal of Computer Science and Technology, 2003, 18(5):553-570.

[9] BURROWS M, ABADI M, NEEDHAMR. A logic of authentication [J]. ACM Transaction in Computer System, 1990, 8(1):18-23.

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

[11] 董军，杨秀娟，赵艳芹.基于串空间模型安全协议形式化分析方法的研究 [J]. 计算机技术的发展，2008，18(04)：051-055.

（收稿日期：2011-09-05）

作者简介：

翁艳琴，女，1985 年生，硕士研究生，主要研究方向：计算机应用和网络信息安全。

石曙东，男，1963 年生，博士，教授，主要研究方向：网络与信息安全。

解颜铭，女，1987 年生，硕士研究生，主要研究方向：信息安全。