文章编号:1001 - 9081(2007)08 - 1915 - 04

一种基于关联规则的安全协议验证方法

胡声洲[1,2],余 敏[1],章志明[1]
(1. 江西师范大学 计算机信息工程学院, 南昌 330022;
2. 赣南师范学院 数学与计算机科学学院, 江西 赣州 341000)
(hushengzhou@sohu.com)

摘 要:提出了一种基于关联规则的安全协议形式化分析方法。从主体认证关联、消息间关联和消息内部关联三个角度去刻画协议,提出了基于以上关联特点的协议验证方法。利用该方法对 Woo and Lam 认证协议进行了逆向验证分析,成功推导出现有的已知攻击路径,使这些已知攻击路径的推导能统一于该验证方法;同时还发现了一个未知的攻击路径,为协议的形式化分析提供了新思路。

关键词:安全协议;关联规则;验证方法
中图分类号: TP309 **文献标志码**:A

Verification method of security protocols based on correlation rules

HU Sheng-zhou[1,2], YU Min[1], ZHANG Zhi-ming[1]
(1. *School of Computer and Information Engineering, Jiangxi Normal University, Nanchang Jiangxi* 330022, *China*;
2. *School of Mathematics and Computer Science, Gannan Normal University, Ganzhou Jiangxi* 341000, *China*)

Abstract: An approach for the formal analysis of security protocols based on the correlation rules was proposed. The character of correlation of protocols was pictured from three aspects: the correlation of authentication between principals, the correlation between messages and within the messages. The verification method was presented based on the above correlation property, which had been used to verify the Woo and Lam authentication Protocol in reverse analysis. Some known attack paths were derived successfully, and made these known attack paths can be derived from this method in unity, and also discovered an unknown attack path. The method provides a new perspective in the formal analysis of the protocols.

Key words: security protocol; correlation rules; verification method

0 引言

安全协议是一种通信协议,是任何安全系统的基础,是实现计算机网络安全的关键。近年来,安全协议的形式化分析是当前该领域的一个研究热点,涌现出大量有效的形式化分析方法,如 BAN 逻辑方法、串空间方法和进程代数方法等。

本文在对已有的安全协议形式化方法的比较分析中发现,协议的关联性反映了协议内部的关联关系,能很好地表达协议的内在语义,同时也是攻击者成功攻击必须利用的重要因素,挖掘协议的关联特点在安全协议的形式化分析中有重大意义。对于这方面的研究, Woo-lam 在文献[1]提出了对应性和保密性的认证特性,但没有严格的形式化描述与分析方法,文献[2]中的通信顺序进程(Communicating Sequential Processes, CSP)方法也沿用了这种对应性作为其协议说明的特性描述,定义了起始和结束事件的前后关联,得到了很好的验证结果,但没有描述每次消息间的关联特点。文献[3]中引入了时态公式来定义这一特性,但在具体分析中又局限于特定步骤的分析。文献[5]中提出了协议相关性这一概念并着手研究,给出了关联因子的一些概念,但仅基于关联因子的形式化分析在刻画协议内涵以及实际应用分析上的力度不足。

本文提出了协议相关性的分析途径,借鉴文献[5]中串空间模型的主体目标绑定思想,同时借鉴文献[6]所提出的一种从攻击者角度考虑的协议形式化分析思路来探索协议的关联特性,形成一定的关联规则并建立基于该规则的协议验证方法,对实际安全协议进行验证分析,提出协议形式化分析的新思路。

1 基于关联性的协议描述

定义 1 主体认证关联是指能反映主体认证关系的一种关联关系,记为 f。相关性是认证协议的基本特征,主体认证可以根据认证方所期待的消息是否得到满足来判定,某个主体认证另外一个主体身份必须接收的消息序列反映了其认证关系。可用下面的公式来表示这种认证关联 f:

$$\text{authen}(B,A): -\langle -Msg1, -Msg2, -Msg3, \cdots\rangle$$

其中 authen(B,A) 表示主体 B 能否认证主体 A,取决于主体 B 是否能依次接收到消息 $Msg1$、$Msg2$、$Msg3$ 等,其中 Msg 前的"-"号表示信息的接收,只有当主体 B 所期待的消息得到满足,主体 B 就认为对方是主体 A。

主体认证关联能很好地描述主体间的关系,强调了认证方接收消息的诚实,放宽对发送消息的限制,适合描述消息发送方的诚实性无法界定这一特点,其形象直观、有利于语义表示。比如对于 B 主体来说,他只能肯定的是他接收了什么消息,至于发送消息的主体具体是谁,在协议运行过程中是无法确定的,也只有成功完成了协议的一次运行实例,即完成一次主体认证关联,它才能认定和其通信的主体是所期待的主体。

收稿日期:2007 - 02 - 15。 **基金项目**: 江西省自然科学基金资助项目(511010)。
作者简介:胡声洲(1975 -),男,江西南康人,讲师,硕士研究生,主要研究方向:信息安全; 余敏(1964 -),女,江西南昌人,教授,主要研究方向:信息安全; 章志明(1978 -),男,江西南昌人,硕士,主要研究方向:信息安全。

以 NS 公钥协议为例，其主体认证关联的描述为：authen(B, A)：$-\langle -\{N_a, A\}k_b, -\{N_b\}k_b\rangle$。其中$\{N_a, A\}k_b$，$\{N_b\}k_b$，是主体 B 认证主体 A 的两个绑定目标，只要能依次接收上述消息，则 B 主体完成对 A 主体的认证。

定义 2 消息之间的关联反映了协议中前后协议步骤中消息之间的关联关系。这种关联关系体现了协议若干条协议步骤的计算能力，称之为消息间规则。该规则反映了协议中每一条规则可获得的消息与协议中前面协议步骤能提供消息之间构成的一种关联关系，是任何主体能生成某种信息的计算器。协议中每一步骤能获得的消息可由该步骤所隐含的消息间规则推出，其一般形式是：$\frac{p_1 p_2 \cdots p_n}{m}$，其中 $p_i (i \in N)$ 和 m 为信息，这个消息间规则表示任何主体只要能提供消息 p_1、p_2、…、p_n，则可以通过前面的协议步骤的计算获得消息 m。每个消息间规则都对应一系列协议步骤来实现主体将信息 $p_1 p_2 \cdots p_n$ 进行装配而得到消息 m，如果该主体是攻击者，则可以据此规则产生攻击者的知识集合，以生成有效的攻击行为。

我们以 Woo-Lam 认证协议来进行说明，Woo-Lam 协议标准描述如下：

$M_1: A \rightarrow B: A$

$M_2: B \rightarrow A: N_b$

$M_3: A \rightarrow B: \{N_b\}k_{as}$

$M_4: B \rightarrow S: \{A, \{N_b\}K_{as}\}k_{bs}$

$M_5: S \rightarrow B: \{N_b\}k_{bs}$

对于第一条协议步骤 $M_1: A \rightarrow B: A$，其消息间规则可表示为：$\overline{A}$，意味着任何主体能从该协议上获得任何希望发起协议会话的主体的身份。与上述规则对应的协议行为是：$A \rightarrow I(B): A$，表示任何主体可在主体 A 对主体 B 发起的协议会话中，截取主体 A 的身份。

对于第二条协议步骤 $M_2: B \rightarrow A: N_b$，相应的规则是：$\frac{A}{N_b}$，表示任何主体通过提供一个发起者身份可以获得一个响应者产生的随机数，其对应的攻击行为是：1) $A \rightarrow I(B): A$；2) $B \rightarrow I(A): N_b$。

定义 3 某主体所获得的未知消息称之为消息未知式，即主体对消息的值、新鲜性和消息的类型均未知。

如 Woo-Lam 认证协议中 $M_2: B \rightarrow A: N_b$ 中的 N_b 就是一个消息未知式，因为 A 在第二步没有用于验证所接收消息是否有效的最初知识，无法验证所收到消息的合法性，同时，N_b 的新鲜性只能由 B 知道，A 不需要第二步中消息的新鲜性。从以上事实可知，A 不知道第二步中所获消息的新鲜性、消息的类型和消息的合法性。

定义 4 消息未知式的变量化是指对于某个主体接收到的消息未知式，可以使用通用的变量代替，表示所接收的消息对于接收者来说可以是任意消息。

上述主体 A 所接收的消息未知式 N_b，对于主体 A 来说相当于获得一个任意的消息。可进行消息未知式的变量化，即用变量 X 代替 N_b，则 Woo-Lam 认证协议可改成如下形式：

$M_1: A \rightarrow B: A$

$M_2: B \rightarrow A: X$

$M_3: A \rightarrow B: \{X\}k_{as}$

$M_4: B \rightarrow S: \{A, \{X\}K_{as}\}k_{bs}$

$M_5: S \rightarrow B: \{N_b\}k_{bs}$

经过消息未知式变量化处理的协议步骤改为 $M_4: B \rightarrow S: \{A, X\}k_{bs}$，其相应的推导规则是：$\frac{AX}{\{A, X\}k_{bs}}$，表示攻击者给出一个主体身份和一个任意的消息，就能获得经 K_{bs} 加密的消息。如果攻击者要冒充主体 A，则可以使用以下攻击脚本：

1) $A(I) \rightarrow B: A$

2) $B \rightarrow I(A): N_b$

3) $I(A) \rightarrow B: X$

4) $B \rightarrow I(S): \{A, X\}K_{bs}$

应用未知消息变量化原理，可以改进该协议的关联特性，如在 Woo-Lam 认证协议的 $M_3: A \rightarrow B: \{N_b\}k_{as}$ 中，B 接收的消息 $\{N_b\}k_{as}$ 就是一个消息未知式，因为由 K_{as} 加密的消息对于主体 B 是不能识别的。经消息变量化后为 $M_3: A \rightarrow B: X$，主体 B 所期待的第二个消息可以是任意消息。由此，上述该协议的主体认证关联可改进为$\langle -A, X, -\{N_b\}k_{bs}\rangle$，第二个期待消息的任意性使主体认证的关联性减弱，降低了协议的安全性。这样，如果攻击者要冒充 A，只要尽力去生成消息 A 和 $\{N_b\}k_{bs}$，就能满足主体 B 的期待而攻击成功。

定义 5 消息内部的关联，指消息自身结构隐含着的一种消息内部的关联。

消息内部关联主要体现在消息的内部结构中，消息结构由消息原子个数、消息原子次序和消息内部主体关系等构成。

消息类型约束在协议形式化描述中很重要，可以定义原子消息，从而构造结构消息，最终描述消息内部的关联关系。消息类型可以表示为：

$TYPEDEF = \{Principal, Key, Nonce, Msg\}$

其中 *Principal* 表示主体，*Key* 表示密钥，*Nonce* 表示随机数，*Msg* 表示消息。

其中构造消息主要有：

消息连接：$\langle Msg1, Msg2, Msg3, \cdots\rangle$

消息加密：

$E((Msg, (Principal, Private)))$：用 *Principal* 的私钥加密消息 *Msg*。

$E((Msg, (Principal, Public)))$：用 *Principal* 的公钥加密消息 *Msg*。

$E((Msg, (Principal1, Principal2)))$：用 *Principal*1 和 *Principal*2 的密钥加密消息 *Msg*。

如：$\{A, \{X\}k_{as}\}k_{bs}$ 表示的是某个主体标识符和用它与服务器的密钥加密的密文连接后，用另一主体和服务器的密钥加密这样一种结构消息，这种消息的结构就隐含着一种消息内部的关联。这个消息的内在关联可描述为：

$Msg = \langle E(\langle Principal1, E(X, (Principal1, S))\rangle, (Principal2, S))\rangle$

此消息间关联表示消息是由主体 2 和密钥服务器的密钥加密的，由主体 1 标识和主体 1 与服务器密钥对任意消息加密后的消息连接而成的。

引入类型比较能很好运用于协议步骤的推导分析，减少状态搜索，更易找出攻击。

2 基于关联规则的协议验证方法

基于以上关联知识，将主体认证关联、消息间关联和消息内部间关联汇合形成关联规则，并根据这些构造规则由目标结果出发逆向分析可能的触发前提，可用以分析协议中可能出现的攻击行为。当然，安全协议环境的一些基本的假设在这里也是适用的。如运行该协议的网络是开放的，任何主体发出的任何消息完全可以被其他主体得到、改变抛弃和替换。攻击者可以是该协议的某个合法主体，它可以发起和参与任意个该协议的运行实例，攻击者可以充分利用该协议本身提

供的计算能力进行攻击。

下面以 Woo-Lam 协议为例,采用基于关联规则的协议验证方法来分析可能出现的攻击行为。

2.1　建立主体的认证关联关系

不失一般性,这里假定是冒充 A 攻击 B,这里只分析主体 B 对主体 A 的认证,也就是要让主体 B 确信和自己通信的是主体 A,主体 B 所需要的认证关联是:

$\langle -A, -X, -\{N_b\}k_{bs}\rangle$

表示 B 主体认证 A,只要依次满足 A,X,$\{N_b\}k_{bs}$ 三个消息的期待要求,则认证成功。其中,主体 B 所期待的第二个消息可以是任意消息。

2.2　消息间关联的推导规则生成

根据 Woo-Lam 认证协议的 M_1、M_2、M_3、M_4 和 M_5 五条协议步骤,可依次产生表 1 所示的消息间关联的五个推导规则和相应的攻击脚本,其中 α 为发起者角色,β 为响应者角色。

表 1　Woo-Lam 认证协议的五个推导规则

序号	推导规则	攻击脚本
R1	$\dfrac{}{\alpha}$	1) $\alpha \rightarrow I(\beta):\alpha$
R2	$\dfrac{\alpha}{N_\beta}$	1) $I(\alpha) \rightarrow \beta:\alpha$ 2) $\beta \rightarrow I(\alpha):N_\beta$
R3	$\dfrac{X}{\{X\}k_{\alpha s}}$	1) $\alpha \rightarrow I(\beta):\alpha$ 2) $I(\beta) \rightarrow \alpha:X$ 3) $\alpha \rightarrow I(\beta):\{X\}k_{\alpha s}$
R4	$\dfrac{\alpha X}{\{\alpha,X\}k_{\beta s}}$	1) $\alpha(I) \rightarrow \beta:\alpha$ 2) $\beta \rightarrow I(\alpha):N_\beta$ 3) $I(\alpha) \rightarrow \beta:X$ 4) $\beta \rightarrow I(S):\{\alpha,X\}K_{\beta s}$
R5	$\dfrac{\{\alpha,\{X\}K_{\alpha s}\}k_{\beta s}}{\{X\}k_{\beta s}}$	1) $I(\beta) \rightarrow S:\{\alpha,\{X\}k_{\alpha s}\}k_{\beta s}$ 2) $S \rightarrow I(\beta):\{X\}k_{\beta s}$

2.3　消息内部关联

结构消息类型主要是 $E((Msg,(Principal, Principal)))$,如 $\{N_b\}k_{bs}$、$\{A,\{X\}K_{as}\}k_{bs}$。在对协议逆向分析比较中,消息内部关联是消息匹配的关键。

2.4　基于关联规则进行协议的逆向验证

为具一般性,这里仍假定攻击者冒充 A 攻击 B,现在利用关联规则推导所有可能的攻击行为,这里限制推导的广度,假设最多有 A、B、C、D 和 E 五个主体参与协议运行:

攻击者要能冒充 A 攻击 B,先从满足第三个期待开始去推导。

2.4.1　主体 B 的第三个期待:$-\{N_b\}K_{bs}$

要求攻击者能得到消息 $\{N_b\}K_{bs}$,然后发送给 B,根据消息间关联关系,进行基于消息内部关联的类型匹配,因为 $\{N_b\}K_{bs}$ 和表 1 所列出规则中的后件 $\{X\}k_{\alpha s}$、$\{\alpha,X\}K_{\beta s}$ 和 $\{X\}k_{\beta s}$ 能进行匹配,此时可用的推导规则有 R3、R4 和 R5。下面就使用这三个规则进行逆向推导:

(1) $\{N_b\}K_{bs} \rightarrow N_b$(利用 R3) $\rightarrow A$(利用 R2) $\rightarrow$ 成立(利用 R1)

$\rightarrow$ wrong(利用 R4,$\{\alpha,X\}K_{\beta s}$ 和 $\{N_b\}K_{bs}$ 类型不匹配)

$\rightarrow$ (1.1) $\{C,\ \{N_b\}k_{cs}\}k_{bs} \mid \{A,\ \{N_b\}k_{as}\}k_{bs} \mid \{D,\{N_b\}k_{ds}\}k_{bs} \mid \{E,\{N_b\}k_{es}\}k_{bs}$(利用 R5,"|" 为或)

(1.1) $\{C,\{N_b\}k_{cs}\}k_{bs} \rightarrow C$,$\{N_b\}k_{cs}$(利用 R3) $\rightarrow$ 类似于 (1) $\rightarrow \{\alpha,\{C,\{N_b\}k_{cs}\}k_{\alpha s}\}k_{bs}$(利用 R5) $\rightarrow$ 限制宽度

这里通过递归推导,可以得到的各种主体组合的攻击者知识:

$\{N_b\}k_{\alpha s}$,$\{\alpha,\{N_b\}k_{\alpha s}\}k_{\beta s}$,$\{\alpha,\{\{\alpha,\{N_b\}k_{\alpha s}\}k_{\beta s}\}k_{\alpha s}\}k_{\beta s}$,$\{\alpha,\{\{\alpha,\{N_b\}k_{\alpha s}\}k_{\beta s}\}k_{\alpha s}\}k_{\beta s}\cdots$

2.4.2　主体 B 的第二个期待:$-X$ 或 $-\{N_b\}k_{as}$

满足 $-X$ 这个期待很容易,满足 $-\{N_b\}k_{as}$ 这个期待类似于 2.4.1 的推导。

2.4.3　主体 B 的第一个期待:$-A$

要求攻击者能得到消息 A,以转发给 B,根据消息类型可知,使用推导规则 1 可满足这个期待,攻击者不必提供任何消息,就能得到 A,攻击场景为:

$A \rightarrow I(B):A$

2.5　选取成功的攻击路径

整理后成功的攻击路径如表 2 所示。

表 2　成功的攻击路径

序号	满足期待	推导路径
攻击一	期待 3	$\{N_b\}k_{bs} \rightarrow N_b$(R3) $\rightarrow A$(R2) $\rightarrow$(R1)
	期待 2	$X \rightarrow X$ 成立
	期待 1	$A \rightarrow$(R1)
攻击二	期待 3、2	$\{N_b\}k_{bs} \rightarrow \{A,\{N_b\}k_{as}\}k_{bs}$(R5) $\rightarrow A$,$\{N_b\}k_{as}$(R4) $\rightarrow \{C,\{N_b\}k_{cs}\}k_{as}$(R5) $\rightarrow C$,$\{N_b\}k_{cs}$(R4) $\rightarrow N_b$(R3) $\rightarrow A$(R2) $\rightarrow$(R1)
	期待 1	$A \rightarrow$(R1)
攻击三	期待 3、2	$\{N_b\}k_{bs} \rightarrow \{A,\{N_b\}k_{as}\}k_{bs}$(R5) $\rightarrow A$,$\{N_b\}k_{as}$(R4) $\rightarrow \{C,\{N_b\}k_{cs}\}k_{as}$(R5) $\rightarrow C$,$\{N_b\}k_{cs}$(R4) $\rightarrow \{D,\{N_b\}k_{ds}\}k_{cs}$(R5) $\rightarrow D$,$\{N_b\}k_{ds}$(R4) $\rightarrow \{E,\{N_b\}k_{es}\}k_{ds}$(R5) $\rightarrow E$,$\{N_b\}k_{es}$(R4) $\rightarrow N_b$(R3) $\rightarrow A$(R2) $\rightarrow$(R1)
	期待 1	$A \rightarrow$(R1)
攻击四	期待 3	$\{N_b\}k_{bs} \rightarrow \{C,\{N_b\}k_{cs}\}k_{bs}$(R5) $\rightarrow \{C,\{C,\{N_b\}k_{cs}\}k_{cs}\}k_{bs}$(R5) $\rightarrow C$,$\{C,\{N_b\}k_{cs}\}k_{cs}$(R4) $\rightarrow C$,$\{N_b\}k_{cs}$(R4) $\rightarrow N_b$(R3) $\rightarrow A$(R2) $\rightarrow$(R1)
	期待 2	$X \rightarrow X$ 成立
	期待 1	$A \rightarrow$(R1)

2.6　攻击场景的合成

1) 攻击 1 的攻击场景:

1.1　$I(A) \rightarrow B:A$

1.2　$B \rightarrow I(A):N_b$

1.3　$I(A) \rightarrow B:X$

1.4　$B \rightarrow I(S):\{X\}k_{bs}$

2.1　$B \rightarrow I(A):B$

2.2　$I(A) \rightarrow B:N_b$

2.3　$B \rightarrow I(A):\{N_b\}k_{bs}$

1.5　$I(S) \rightarrow B:\{N_b\}k_{bs}$

2）攻击 2 的攻击场景：

1.1 $I(A) \rightarrow B:A$

1.2 $B \rightarrow I(A):N_b$

2.1 $C \rightarrow I(B):C$

2.2 $I(B) \rightarrow C:N_b$

2.3 $C \rightarrow I(B):\{N_b\}k_{cs}$

3.1 $A \rightarrow I(C):A$

3.2 $I(C) \rightarrow A:C,\{N_b\}k_{cs}$

3.3 $A \rightarrow I(C):\{C,\{N_b\}k_{cs}\}k_{as}$

4.1 $I(A) \rightarrow S:\{C,\{N_b\}k_{cs}\}k_{as}$

4.2 $S \rightarrow I(A):\{N_b\}k_{as}$

1.3 $I(A) \rightarrow B:A,\{N_b\}k_{as}$

1.4 $B \rightarrow S:\{A,\{N_b\}k_{as}\}k_{bs}$

1.5 $S \rightarrow B:\{N_b\}k_{bs}$

3）攻击 3 的攻击场景：

1.1 $I(A) \rightarrow B:A$

1.2 $B \rightarrow I(A):N_b$

2.1 $E \rightarrow I(B):E$

2.2 $I(B) \rightarrow E:N_b$

2.3 $E \rightarrow I(B):\{N_b\}k_{es}$

3.1 $D \rightarrow I(E):D$

3.2 $I(E) \rightarrow D:E,\{N_b\}k_{es}$

3.3 $D \rightarrow I(E):\{E,\{N_b\}k_{es}\}k_{ds}$

4.1 $I(D) \rightarrow S:\{E,\{N_b\}k_{es}\}k_{ds}$

4.2 $S \rightarrow I(D):\{N_b\}k_{ds}$

5.1 $C \rightarrow I(D):C$

5.2 $I(D) \rightarrow C:D,\{N_b\}k_{ds}$

5.3 $C \rightarrow I(D):\{D,\{N_b\}k_{ds}\}k_{cs}$

5.4 $I(C) \rightarrow S:\{D,\{N_b\}k_{ds}\}k_{cs}$

5.5 $S \rightarrow I(C):\{N_b\}k_{cs}$

6.1 $A \rightarrow I(B):A$

6.2 $I(B) \rightarrow A:C,\{N_b\}k_{cs}$

6.3 $A \rightarrow I(B):\{C,\{N_b\}k_{cs}\}k_{as}$

7.1 $I(C) \rightarrow S:\{C,\{N_b\}k_{cs}\}k_{as}$

7.2 $S \rightarrow I(A):\{N_b\}k_{as}$

1.3 $I(A) \rightarrow B:A,\{N_b\}k_{as}$

1.4 $B \rightarrow S:\{A,\{N_b\}k_{as}\}k_{bs}$

1.5 $S \rightarrow B:\{N_b\}k_{bs}$

4）攻击 4 的攻击场景：

1.1 $I(A) \rightarrow B:A$

1.2 $B \rightarrow I(A):N_b$

1.3 $I(A) \rightarrow B:A,X$

1.4 $B \rightarrow S:\{A,X\}k_{bs}$

2.1 $C \rightarrow I(D):C$

2.2 $I(D) \rightarrow C:N_b$

2.3 $C \rightarrow I(D):\{N_b\}k_{cs}$

3.1 $C \rightarrow I(B):C$

3.2 $I(B) \rightarrow C:C,\{N_b\}k_{cs}$

3.3 $C \rightarrow I(B):\{C,\{N_b\}k_{cs}\}k_{cs}$

4.1 $B \rightarrow I(C):B$

4.2 $I(C) \rightarrow B:C,\{C,\{N_b\}k_{cs}\}k_{cs}$

4.3 $B \rightarrow I(C):\{C,\{C,\{N_b\}k_{cs}\}k_{cs}\}k_{bs}$

4.4 $I(B) \rightarrow S:\{C,\{C,\{N_b\}k_{cs}\}k_{cs}\}k_{bs}$

4.5 $S \rightarrow I(B):\{C,\{N_b\}k_{cs}\}k_{bs}$

5.4 $I(B) \rightarrow S:\{C,\{N_b\}k_{cs}\}k_{bs}$

5.5 $S \rightarrow I(B):\{N_b\}k_{bs}$

1.5 $I(S) \rightarrow B:\{N_b\}k_{bs}$

其中攻击 1、2、4 与文献[6]中是一致的，而攻击 3 是一个新的攻击路径。

3 结语

通过对 Woo-Lam 协议的具体分析，基于关联规则能够很好地分析基于重放攻击的攻击行为，在检验过程中，能通过使用关联规则统一推导出现有的已知攻击，并能发现新的攻击（如攻击 3）。从以上推导过程中可以看出，存在许多向外扩张的推导步骤，这反映了协议的攻击路径具有无穷性。该协议中规则 5 可使推导更为复杂，而规则 3 和 4 则使推导向更为简单的方向发展，规则 1 和 2 则是攻击者成功攻击必须使用的规则，即是攻击者成功攻击的终点位置。很容易看出，只要用规则 5 往更深方向推导，参与协议的主体无限，则复杂的攻击场景将有无穷多个，其攻击行为的个数也是无限的。

协议的关联性是安全协议的基本特征，开展对协议的关联特性的研究和创新，完善安全协议的关联性理论和基于关联规则的协议验证方法，对提高安全协议的分析能力有重要的作用。

参考文献：

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

[2] HORE C A R. Communicating sequential processes [M]. New Jersey: Prentice-Hall, 1985.

[3] 丁一强. 基于 CCS 的加密协议分析[J]. 软件学报, 1999, 10(10): 1103 - 1107.

[4] 梁坚. 密码协议验证与设计中若干关键技术研究[D]. 上海: 上海交通大学电子信息学院, 2001.

[5] 周宏斌, 黄连生, 桑田. 基于串空间的安全协议形式化验证模型及算法[J]. 计算机研究与发展, 2003, 40(2): 251 - 256.

[6] DEBBABI M, MEJRI M, TAWBI N, *et al*. A new algorithm for the automatic verification of authentication protocols: from specifications to flaws and attack scenarios[EB/OL]. [2007 - 01 - 03]. http://dimacs.rutgers.edu/Workshops/Security/program2/debbabi/index.html

（上接第 1914 页）

参考文献：

[1] BLAKEY G R. Safeguarding cryptographic keys[C]// Proceedings of NCC. Montvale: AFIPS Press, 1979, 48: 313 - 317.

[2] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 24(11): 612 - 613.

[3] HE J, DAWSON E. Multi stage secret sharing based on one way function[J]. Electronics Letters, 1994, 30(19): 1591 - 1592.

[4] HE J, DAWSON E. Multi secret sharing scheme based on one way function[J]. Electronics Letters, 1995, 31(2): 93 - 95.

[5] HAM L. Comment: multi stage secret sharing based on one-way function[J]. Electronics Letters, 1995, 31(4): 262 - 263.

[6] HAM L. Efficient sharing (broadcasting) of multiple secrets[J]. IEE Proceedings of Computers and Digital Techniques, 1995, 142(3): 237 - 240.

[7] CHIEN H Y, JAN J K, TSENG Y M. A practical (t, n) multi secret sharing scheme[J]. IEICE Transactions on Fundamentals, 2000, E83-A(12): 2762 - 2765.

[8] 庞辽军, 柳毅, 王育民. 一个有效的(t, n)门限多重秘密共享体制[J]. 电子学报, 2006, 34(4): 587 - 589.

[9] 李滨. 基于特殊访问权限的差分秘密共享方案[J]. 四川大学学报: 自然科学版, 2006, 43(1): 78 - 83.