基于广义串空间模型构造攻击的缺陷及改进

王建华[①]　张　岚[②]　何良生[②]　许　旸[③]
[①](北京航空航天大学计算机学院　北京　100083)
[②](解放军信息工程大学电子技术学院　郑州　450004)
[③](空军电子技术研究所　北京　100097)

摘　要：该文设计一个类似于Millen曾经构造的“ffgg”协议——“ffgg*”协议，它们有共同的密码学性质。使用基于广义串空间模型的构造攻击对该协议进行分析，结果表明协议在非类型缺陷攻击下是安全的，这与Millen用Pulson的归纳法分析“ffgg”协议有相同的结果，并指出该方法是有缺陷的。针对这个缺陷，给出改进的措施，改进的构造攻击能发现“ffgg*”协议中的类型缺陷攻击。

关键词：构造攻击；广义串空间模型；“ffgg”协议
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2007)10-2451-04

Flaws and Improvement on Constructing Attack Based on Generalized Strand Space Model

Wang Jian-hua[①]　Zhang Lan[②]　He Liang-sheng[②]　Xu Yang[③]
[①](*School of Computer Science*, *Beijing University of Aeronautics and Astronautics*, *Beijing* 100083, *China*)
[②](*Institude of Electronic Technology*, *the PLA Information Engineering University*, *Zhengzhou* 450004, *China*)
[③](*Institute of Electronic Technology*, *Air Force*, *Beijing* 100097, *China*)

Abstract: This paper designs “ffgg*” protocol which is similar to“ffgg” protocol constructed by Millen.They have cryptographic properties in commen. Then,the protocol is analyzed by using constructing attack based on generalized strand space model ,and it is proved that the protocol is secure under non-type-flaw attacks .After “ffgg” protocol is analyzed by Millen using Pulsons inductive approach,it is secure under non-type-flaw attacks,either. It is indicated that constructing attack has limitation. Finally,some improved measures are put forward,and type-flaw attack is found by using amendatory constructing attack in “ffgg*” protocol.

Key words: Constructing attack；Generalized strand space model；“ffgg” protocol

1　引言

基于广义串空间模型的构造攻击在寻找密码协议的漏洞方面已显示出极大的成功[1, 2]，然而，一个模型分析方法未能发现密码协议的缺陷，并不能说明该方法就是完善的，基于广义串空间模型的构造攻击就是如此。Millen曾利用Paulson的归纳法[3]证明“ffgg”[4]是安全的。其实此协议是不安全的，存在类型缺陷攻击。为了说明基于广义串空间模型的构造攻击存在同样的问题，本文设计了一个类似“ffgg”的协议——“ffgg*”协议，它们有共同的密码学性质。

基于广义串空间模型的构造攻击[2]由中科院软件所季庆光等提出的，对一个实体认证协议[2]作了深入的分析，发现了协议中存在的类型缺陷攻击，攻击的结果只使协议的认证性目标失效，协议的秘密性目标是成立的。在“ffgg*”中，使用基于广义串空间模型的构造攻击分析，两个目标都是成立的。实事上，秘密性目标是不成立的，因为类型缺陷攻击的结果使秘密的会话密钥泄露了，这说明基于广义串空间模型的构造攻击是有缺陷的。针对这种缺陷，本文给出了改进的措施。

2006-04-03 收到，2007-05-08 改回

2　“ffgg*”协议

(1) $A \to B : A, N_2$；(2) $B \to A : B, N_1, N_2$；
(3) $A \to B : A, \{N_1, N_2, K_{AB}\}_{\mathrm{PKB}}$；(4) $B \to A : N_1, N_2, \{N_2, K_{AB}, N_1\}_{\mathrm{PKB}}$。

协议的最终目标是在主体 A 与 B 之间建立一个共享密钥 K_{AB}。

定义 1 两方广义串空间是一个渗透串空间 Σ，$\Sigma = \Sigma_{\mathrm{Init}} \cup \Sigma_{\mathrm{Resp}} \cup P \cup \Sigma_{\mathrm{Oracle}}$。其中：

(1) $\mathrm{Init}[A, B, N_1, N_2, K_{AB}]$ 是如下串 $s \in \Sigma$ 的集合，它的迹为 $\langle +\{A, N_2\}, -\{B, N_1, N_2\}, +\{A, \{N_1, N_2, K_{AB}\}_{\mathrm{PKB}}\}, -\{N_1, N_2, \{N_2, K_{AB}, N_1\}_{\mathrm{PKB}}\}\rangle$，$\Sigma_{\mathrm{Init}}$ 是 $\mathrm{Init}[A, B, N_1, N_2, K_{AB}]$ 的联合。

(2) $\mathrm{Resp}[A, B, N_1, N_2, K_{AB}]$ 是如下串 $s \in \Sigma$ 的集合，它的

迹为
$\left\langle -\{A,N_2\},+\{B,N_1,N_2\},-\left\{A,\{N_1,N_2,K_{AB}\}_{PKB}\right\},+\{N_1,N_2,\{N_2,K_{AB},N_1\}_{PKB}\}\right\rangle$， Σ_{Resp} 是 $\text{Resp}[A,B,N_1,N_2,K_{AB}]$ 的联合。

(3)攻击者串 P 是由攻击者原子行为迹[6]组成的。

(4) $\text{Oracle}[A,B,N_1,N_2,K_{AB}]$ 是如下串 $s\in\Sigma$ 的集合，它的迹为
$\left\langle -\{A,X\}\right\rangle$；$\left\langle -\{A,X\},+\{B,N_1,X\}\right\rangle$；$<-\{A,X\},+\{B,N_1,X\},-\{A,\{N_1,X,\ K_{AB}\}_{\text{PKB}}>$；$<-\{A,X\},+\{B,N_1,X\},-\left\{A,\{N_1,X,K_{AB}\}_{\text{PKB}}\right\},+\{N_1,X,\{X,\ K_{AB},N_1\}_{\text{PKB}}\}>$。$\Sigma_{\text{Oracle}}$ 是 $\text{Oracle}[A,B,N_1,N_2,K_{AB}]$ 的联合。

3 协议攻击分析

命题 1 若 Σ 是一个两方协议串空间， C 是 Σ 中的一个丛， $\text{PKB}^{-1}\notin K_P$， K_P 是攻击者已知的密钥集合，则对 $\forall m\in C,\text{PKB}^{-1}\not\subset\text{uns-term}(m)$。

证明 因为 PKB^{-1} 不在常规节点源发，所以证明与文献[5]中的命题 3.3 类似。

命题 2 假设 Σ 是一个两方协议串空间， C 是 Σ 中的一个丛。若下面的条件满足：

(1) s 是一个响应者串，在 $\text{Resp}[A,B,N_1,N_2,K_{AB}]$ 中具有 C-height 4；

(2) $\text{PKB}^{-1}\notin K_P$；(3) N_1 在 Σ 中唯一源发。

则 C 或包含一个始发者串具有 C-height 4，或包含一个响应者串具有 C-height 4：
$\left\langle -\{A,N_2\},+\{B,N_1,N_2\},-\left\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\right\},+\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\text{PKB}}\}\right\rangle$。

证明 假定 s 是 $<-\{A,N_2\},+\{B,N_1,N_2\},-\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\},+\{N_1,N_2,\ \{N_2,K_{AB},N_1\}_{\text{PKB}}\}>$， $N_1\subset\text{term}(\langle s,2\rangle)$，且 N_1 在 $\langle S,2\rangle$ 源发。令 $S=\{n\in C:\{N_2,K_{AB},N_1\}_{\text{PKB}}\subset\text{uns-term}(n)\}$。因为 $\{N_2,K_{AB},N_1\}_{\text{PKB}}\subset\text{uns-term}(\langle s,4\rangle)$，所以 $\langle s,4\rangle\in S$。因此 S 非空。由极小元原理可知，集合 S 中有一个极小元 n_1，且 $\{N_2,K_{AB},N_1\}_{\text{PKB}}\subset\text{uns-term}(n_1)$，$n_1$ 的符号是正的。

经过验证，可知 n_1 不在入侵者原子行为迹[6]上，因此 n_1 一定在常规者串上。不妨设此常规者串为 T。因为 N_1 不源于节点 n_1，所以节点 n_1 不是 $I=\{n:N_1\subset n\}$ 的入口点，由入口点的定义可知，在常规者串 T 上节点 n_1 之前一定存在一个节点 n_2，且 $N_1\subset\text{term}(n_2)$，$n_2<n_1$。若包含节点 n_1 与 n_2 的常规者串 T 是始发者串，根据始发者串的一般形式：$\left\langle +\{C,N_2\},-\left\{D,N_1',N_2'\right\},+\left\{C,\left\{N_1',N_2',K_{AB}'\right\}_{\text{PKD}}\right\},-\left\{N_1',N_2',\left\{N_2',K_{AB}',N_1'\right\}_{\text{PKD}}\right\}\right\rangle$ 以及节点 n_1 与 n_2 的特点可得：$\left\{N_1',N_2',K_{AB}'\right\}_{\text{PKD}}=\{N_2,K_{AB},N_1\}_{\text{PKB}}$，由公理 1[7]可知：$\text{PKD}=\text{PKB},N_1'=N_2,N_2'=K_{AB},K_{AB}'=N_1$。所以常规者串 T 为 $<+\{C,K_{AB}\},-\{D,N_2,\ K_{AB}\},+\{C,\{N_2,K_{AB},N_1\}_{\text{PKB}}\},-\left\{N_2,K_{AB},\{K_{AB},N_1,N_2\}_{\text{PKB}}\right\}>$，$\text{term}(n_1)=+\{C,\{N_2,K_{AB},N_1\}_{\text{PKB}}\}$，$\text{term}(n_2)=+\{C,K_{AB}\}$ 或者 $\text{term}(n_2)=-\{D,N_2,K_{AB}\}$，但是，$N_1\not\subset\text{term}(n_2)$，这与上述结论矛盾，所以这个伪正规者串不符合要求，应舍去；若包含节点 n_1 与 n_2 的常规串 T 是响应者串，根据响应者串的一般形式 $<-\left\{C,N_2'\right\},+\left\{D,N_1',N_2'\right\}$， $-\left\{C,\left\{N_1',N_2',K_{AB}'\right\}_{\text{PKD}}\right\},+\left\{N_1',N_2',\left\{N_2',K_{AB}',N_1'\right\}_{\text{PKD}}\right\}>$ 以及节点 n_1 与 n_2 的特点可得：$\left\{N_2',K_{AB}',N_1'\right\}_{\text{PKD}}=\{N_2,K_{AB},N_1\}_{\text{PKB}}$，由公理 1[7]可知：$\text{PKD}=\text{PKB},N_2'=N_2$， $K_{AB}'=K_{AB},N_1'=N_1$。所以常规者串 T 为：$<-\{C,N_2\},+\{D,N_1,N_2\},-\{C,\{N_1,N_2\ ,K_{AB}\}_{\text{PKB}}\},+\left\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\text{PKB}}\right\}>$。由于 T 串是常规响应者串，所以串 T 中的始发者和响应者均已确定，即：$C=A,D=B$。所以 T 串是：$<-\{A,N_2\},+\{B,N_1,N_2\},-\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\},+\left\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\text{PKB}}\right\}>$。因此通过基于广义串空间模型构造攻击构造出来的伪正规串为 $<-\{A,N_2\},+\{B,N_1,N_2\},-\left\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\right\}+\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\text{PKB}}\}>$。

这种伪正规串满足认证的规约[5]，是一次有效的协议运行。 证毕

命题 3 假设 Σ 是一个两方协议串空间， C 是 Σ 中的一个丛。若下面的条件满足：

(1) s 是一个始发者串，在 $\text{Init}[A,B,N_1,N_2,K_{AB}]$ 中具有 C-height 4；

(2) $\text{PKB}^{-1}\notin K_P$；(3) N_2 在 Σ 中唯一源发。

则 C 或包含一个响应者串具有 C-height 4，或包含一个始发者串具有 C-height 4：
$\left\langle +\{A,N_2\},-\{B,N_1,N_2\},+\left\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\right\},-\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\text{PKB}}\}\right\rangle$。

证明 假定 s 是 $<+\{A,N_2\},-\{B,N_1,N_2\},+\{A,\{N_1,N_2,K_{AB}\}_{\text{PKB}}\},-\{N_1,N_2\ ,\{N_2,K_{AB},N_1\}_{\text{PKB}}>$，$N_2\subset\text{term}(\langle s,1\rangle)$，且 N_2 在 $\langle s,1\rangle$ 源发。令 $S=\{n\in C:\{N_1,N_2\ ,K_{AB}\}_{\text{PKB}}\subset\text{uns-term}(n)\}$。因为 $\{N_1,N_2,K_{AB}\}_{\text{PKB}}\subset\text{uns-term}(\langle s,3\rangle)$，所以 $\langle s,3\rangle\in S$。因此 S 非空。由极小元原理可知，集合 S 中有一个极小元 n_1，且 $\{N_1,N_2,K_{AB}\}_{\text{PKB}}\subset\text{uns-term}(n_1)$，$n_1$ 的符号是正的。

经过验证可知， n_1 不在入侵者原子行为迹[6]上，因此 n_1 一定在常规者串上。不妨设此常规者串为 T。因为 N_2 不源于节点 N_1，所以节点 N_1 不是 $I=\{n:N_2\subset n\}$ 的入口点，由入口点的定义可知，在常规者串 T 上节点 n_1 之前一定存在一个节点，不妨设为 n_2，且 $N_2\subset\text{term}(n_2)$，$n_2<n_1$。若包含节点 n_1 与 n_2 的常规者串 T 是始发者串，根据始发者串的一

般形式：$<+\{C,N_2'\},-\{D,N_1',N_2'\},+\{C,\{N_1',N_2',K_{AB}'\}_{\mathrm{PKD}}\},-\{N_1',N_2',\{N_2',K_{AB}',N_1'\}_{\mathrm{PKD}}>$以及节点 n_1 与 n_2 的特点可得：$\{N_1',N_2',K_{AB}'\}_{\mathrm{PKD}}=\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}$，由公理 1[7]可知：$\mathrm{PKD}=\mathrm{PKB},N_1'=N_1,N_2'=N_2,K_{AB}'=K_{AB}$。所以常规者串 T 为 $\langle+\{C,N_2\},-\{D,N_1,N_2\},+\{C,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\},-\{N_1,N_2,\{N_2,K_{AB},N_1\}_{\mathrm{PKB}}\}\rangle$，由于 T 串是常规始发者串，所以串 T 的始发者和响应者均已确定，即 $C=A,D=B$，所以 T 串为：$\langle+\{A,N_2\},-\{B,N_1,N_2\},+\{A,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\},-\{N_1,N_2,\{N_2,K_{AB},N_1\}\}\rangle$；若包含节点 n_1 与 n_2 的常规者串 T 是响应者串，根据响应者串的一般形式 $<-\{C,N_2'\},+\{D,N_1',N_2'\},-\{C,\{N_1',N_2',K_{AB}'\}_{\mathrm{PKD}}\},+\{N_1',N_2',\{N_2',K_{AB}',N_1'\}_{\mathrm{PKD}}\}>$以及节点 n_1 与 n_2 的特点可得：$\{N_2',K_{AB}',N_1'\}_{\mathrm{PKD}}=\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}$，由公理 1[5]可知：$\mathrm{PKD}=\mathrm{PKB},N_2'=N_1$，$K_{AB}'=N_2,N_1'=K_{AB}$。所以常规者串 T 为：$<-\{C,N_1\},+\{D,K_{AB},N_1\},-\{A,\{K_{AB},N_1,N_2\}_{\mathrm{PKB}}\},+\{K_{AB},N_1,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\}>$。由于 T 串是常规响应者串，所以串 T 中的始发者和响应者均已确定，即 $C=A,D=B$。所以 T 串是：$<-\{A,N_1\},+\{B,K_{AB},N_1\},-\{A,\{K_{AB},N_1,N_2\}_{\mathrm{PKB}}\},+\{K_{AB},N_1,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\}>$。因此基于广义串空间模型构造攻击构造的伪正规串有两种：(1) $<+\{A,N_2\},-\{B,N_1,N_2\},+\{A,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\},-\{N_1,N_2\{N_2,K_{AB},N_1\}_{\mathrm{PKB}}\}>$；(2) $<-\{A,N_1\},+\{B,K_{AB},N_1\}-\{A,\{K_{AB},N_1,N_2\}_{\mathrm{PKB}}\}+\{K_{AB},N_1,\{N_1,N_2,K_{AB}\}_{\mathrm{PKB}}\}>$。

下面分析这两种伪正规串是否为有效的协议运行。第(1)种伪正规串满足认证的规约[5]，是一次有效的协议运行；第(2)种伪正规串，在第 2 步时发送了一条包含会话密钥 K_{AB} 的消息 $\{B,K_{AB},N_1\}$，不妨设为 n_3，即 $\mathrm{term}(n_3)=+\{B,K_{AB},N_1\}$，由于会话密钥 K_{AB} 在常规者串上节点里不以明文的方式发送，所以 n_3 不可能位于常规者串上，则 n_3 一定位于入侵者串上，同样得验证入侵者原子行为迹[6]，经过验证，n_3 不可能位于入侵者串[6]上。因此，第(2)种伪正规串不存在，应舍去。　　证毕

综上所述，基于广义串空间模型的构造攻击对上述认证协议所做的攻击分析表明，使用构造攻击找不出上述协议的缺陷。但是，上述协议确实存在类型缺陷攻击，基于广义串空间模型的构造攻击是不完善的。

4　基于广义串空间模型构造攻击的完善

4.1 基于广义串空间模型构造攻击的缺陷

考察以上对“ffgg★”协议的分析过程，就可以发现构造攻击方法不能发现类型缺陷攻击的原因主要是分析过程的问题，在确定了包含测试元素的极小元不在攻击者串上而在常规者串上后，没有继续对这个极小元节点以后的发送和接收情况作深入的分析。

4.2 基于广义串空间模型构造攻击的改进

参考文献[8]对认证测试的修改，对基于广义串空间模型的构造攻击改进如下：

假设节点 n 的运行主体是 P，则在应用构造攻击的过程中，包含测试元素 t 的极小元节点值发出后可能被除 P 外的其他常规主体接收到，也可能被 P 接收到。如果被除 P 外的其他常规主体接收到，并将解密后的值以新的加密形式传递给 P，则证明过程同文献[2]；如果被 P 接收到，则需作如下检查：如果遵循协议规则运行的 P 中存在另外一个节点，包含测试元素 t'，且 t 中各个子项的数据位数与 t' 中对应的各个子项的数据位数相同，那么就需要检验该协议中是否存在类型错误攻击。

可以通过以下 3 个步骤检查是否存在类型错误攻击：

(1)确定 P 发送包含测试元素 t 的节点值所在串 s_1；

(2)确定 P 收到并解密包含测试元素 t 的节点值所在的串 s_2；

(3)由这两个串确定攻击串。

分析完命题 2 后得到一个伪正规串，通过检查，发现协议主体 B 的串中节点 $\langle s_{B\_1},3\rangle$ 与 $\langle s_{B\_2},4\rangle$ 中的加密成分，对应的各个子项的数据位数均相同，因此符合需要检测是否存在类型错误攻击的条件。下面作具体的分析：

根据协议的随机数唯一源发和基于广义串空间模型的构造攻击，串 s_1 中含有包含随机数 N_1 的极小元节点值，且 N_1 在 $\langle s_1,2\rangle$ 唯一源发，所以有

$$s_1=<-\{C,X_2\},+\{D,N_1,X_2\}-\{C,\{N_1,X_2',K_{CD}\}_{\mathrm{PKB}}\}+\{N_1,X_2',\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}\}> \tag{1}$$

且发送包含测试元素 $t=\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}$ 的极小元节点值 $\{N_1,X_2',\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}\}$。

因为串 s_1 对应的常规主体是响应者 B，所以 $D=B$；主体 C 与在节点 $\langle s_{B\_1},4\rangle$ 中用的加密密钥对应的主体标志符相同，而共享密钥 PKB 的主体只有 A 与 B，所以 $C=A$。X_2 是主体 A 产生的随机数，以明文的形式发送出去，所以串 s_1 的节点 $\langle s_{B\_1},3\rangle$ 的加密消息成分 X_2' 不一定与 X_2 相同。所以串 s_1 修改为

$$s_1=<-\{A,X_2\},+\{B,N_1,X_2\},-\{A,\{N_1,X_2',K_{CD}\}_{\mathrm{PKB}}\}+\{N_1,X_2',\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}\}> \tag{2}$$

对于 s_2 的一般形式：

$$s_2=<-\{C',X_4\},+\{D',X_3,X_4\}-\{C',\{X_3,X_4',K_{CD}'\}_{\mathrm{PKB}}\}+\{X_3,X_4',\{X_4',K_{CD}',X_3\}_{\mathrm{PKB}}\}> \tag{3}$$

因为 s_2 串收到并解密了测试元素 $\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}$，所以由协议的要求可知：$\{X_2',K_{CD},N_1\}_{\mathrm{PKB}}=\{X_3,X_4',$

$K'_{CD}\}_{\mathrm{PKB}}$，由公理 1[1]可得，$X_3 = X'_2, X'_4 = K_{CD}, K'_{CD} = N_1$。因为串 s_2 对应的常规主体是响应者 B，所以 $D' = B$；因为主体 C' 与在节点 $\langle s_{B\_2}, 4\rangle$ 中用的加密密钥 PKB 对应的主体标志符相同，而共享密钥 PKB 的主体只有 A 与 B，所以 $C' = A$。又因为 X_4 是主体 A 产生的随机数，以明文的形式发送出去，所以串 s_2 的节点 $\langle s_{B\_2}, 3\rangle$ 中的加密消息成分 X'_4 不一定与 X_4 相同。所以串 s_2 修改为

$$s_2 = < -\{A, X_4\}, +\{B, X'_2, X_4\} - \{A, \{X'_2, K_{CD}, N_1\}_{\mathrm{PKB}}\} + \{X'_2, K_{CD}, \{K_{CD}, N_1, X'_2\}_{\mathrm{PKB}}\} > \quad (4)$$

因为 X_2, X_4 分别是 B_1 与 B_2 协议中始发者产生的随机数，不妨设为 $X_2 = N_2, X_4 = N'_2$；又因为 X'_2 是 B_2 产生的随机数，不妨设为 $X'_2 = N'_1$；在式(2)中，K_{CD} 是始发者 A 产生的用于 A 与 B 通话的会话密钥，所以 $K_{CD} = K_{AB}$。串 s_1 与 s_2 修改为

$$s_1 = < -\{A, N_2\}, +\{B, N_1, N_2\}, -\{A, \{N_1, N'_1, K_{AB}\}_{\mathrm{PKB}}\} + \{N_1, N'_1, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\} > \quad (5)$$

$$s_2 = < -\{A, N'_2\}, +\{B, N'_1, N'_2\} - \{A, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\} + \{N'_1, K_{AB}, \{K_{AB}, N_1, N'_1\}_{\mathrm{PKB}}\} > \quad (6)$$

至此，我们得到了已经确定好的串 s_1 (式(5))与串 s_2 (式(6))，可根据这两个并发串的行为确定攻击者串。具体过程如下：

协议开始后，串 s_1 在 $\langle s_{B\_1}, 1\rangle$ 收到了始发者 A 发送的 $\{A, N_2\}$；与此同时，串 s_2 在 $\langle s_{B\_2}, 1\rangle$ 收到了攻击者 P 假冒 A 发送的 $\{A, N'_2\}$，B_1 产生消息 $\{B, N_1, N_2\}$ 来响应，不过这个消息被攻击者 P 截获，B_2 产生消息 $\{B, N'_1, N'_2\}$ 来响应。攻击者收到这两条消息后，产生消息 $\{B, N_1, N'_1\}$ 冒充 B_1 来响应 A，A 根据协议要求，产生 $\{A, \{N_1, N'_1, K_{AB}\}_{\mathrm{PKB}}\}$ 发送给 B_1，B_1 根据协议的要求，产生 $\{N_1, N'_1, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\}$ 发送给 A，在传送过程中被攻击者 P 截获，根据协议的要求，P 假冒 P 产生 $\{A, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\}$ 发送给 B_2，根据协议的要求，B_2 产生 $\{N'_1, K_{AB}, \{K_{AB}, N_1, N'_1\}_{\mathrm{PKB}}\}$ 发送给 A，被攻击者 P 截获。至此，可以得出攻击者的串为：$< +\{A, N'_2\}, -\{B, N_1, N_2\}, -\{B, N'_1, N'_2\}, +\{B, N_1, N'_1\}, -\{N_1, N'_1, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\}, +\{A, \{N'_1, K_{AB}, N_1\}_{\mathrm{PKB}}\}, -\{N'_1, K_{AB}, \{K_{AB}, N_1, N'_1\}_{\mathrm{PKB}}\} >$ 这种形式的类型缺陷攻击描述如图 1 所示。

由上述的分析可以看到，改进的基于广义串空间模型的构造攻击能分析出“ffgg*”协议存在的类型缺陷攻击，说明改进措施是有效的。

5 结束语

本文以“ffgg*”协议为例，指出了基于广义串空间模型构造攻击的缺陷，给出了相应的修正措施。修正后的构造攻击能发现隐藏在“ffgg*”协议中的类型缺陷攻击，这说明修正措施是有效的。

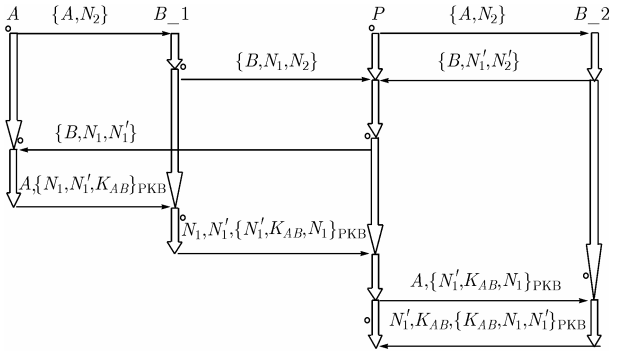

图 1 类型图错误攻击

参 考 文 献

[1] 季庆光. 广义 Strand Space 理论及其应用. 信息安全国家重点实验室安全协议研讨会文集, 2004 年 10 月: 179- 201. LOIS. http://www.is.ac.cn

[2] Ji Qingguang, Qing Sihan, Zhou Yongbin, and Feng Dengguo. Study on strand space model theory. *J. Comput, Sci. & Technol,* 2003, 18(5): 553-570.

[3] Paulson L C. Proving properties of security protocols by induction.in 10th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1997: 70-83.

[4] Millen J K. A necessarily parallel attack, In FLoC Workshop on Formal Methods and Security Protocols, 1999. http://citeseer. ist. psu. edu/millen99necessarily. html

[5] Lowe G. A hierarchy of authentication specifications.In Proc.The 10th Computer Security Foundation Workshop, Rockport, Massachusetts, USA, 1997: 31-43.

[6] Dolev D and Yao A. On the security of public key protocols. *IEEE Trans. on Information Theory*, 1983, 29(2): 198-208.

[7] Fabrega F J T, Herzog. J C, and Guttman J D. Strand space: Proving security protocols correct. *Journal of Computer Security*, 1999, 7(2/3): 191-230.

[8] 邓珍荣. 基于串空间模型的协议验证技术研究.[硕士论文], 广西大学, 2005.

王建华： 男，1962 年生，高级工程师，博士，主要研究方向为信息安全.

张 岚： 男，1978 年生，硕士，研究方向为应用数学、密码理论与形式化方法.

何良生： 男，1963 年生，研究员，博士，主要研究方向为密码理论.

许 旸： 男，1974 年生，硕士，研究方向为信息安全.