基于认证测试的一种安全协议一致性分析方法*)

周清雷　王　峰　赵东明

(郑州大学信息工程学院　郑州 450052)

摘　要　认证测试[1]技术是串空间(strand space)理论的进一步发展,不仅用于认证协议的安全性分析而且还用于指导认证协议的设计[2]。但在分析安全协议为何不正确以及如何改进方面,与其他的形式化验证方法一样,也不能提供更深入有效的分析。本文提出了参数一致性矩阵的概念并运用参数一致性矩阵对协议的一致性进行分析,说明了协议失败的原因并给出改进的方向。分析过程的形式化有利于协议分析自动化工具的实现。

关键词　认证测试,安全协议,串空间模型,一致性

An Agreement Analysis Method of Security Protocol Based on Authentication Test

ZHOU Qing-Lei　WANG Feng　ZHAO Dong-Ming

(School of Information Engineering, Zhengzhou University ,Zhengzhou 450052)

Abstract　Authentication Test is the further development of strand space, it can be used not only for analyzing protocols, but also for guiding the design of protocol. However in the aspect of why a protocol is incorrect and how to improve it, Authentication Test can not offer deeper and more effective analysis as other formal methods. This paper put forward the concept of the parameter-agreement-matrix, carry on deep analysis to the agreement property of protocol, well solve this problem. In addition, the formal process make protocol analysis automatically.

Keywords　Authentication test, Security protocol, Strand space model, Agreement property

1　引言

安全协议是网络安全的一个重要组成部分,它的形式化分析已经逐渐成为信息安全研究领域中的一个热点。1998年,Fabrega, Herzog 和 Guttman 提出了串空间模型[3],将安全协议的形式化分析技术推向一个新的高度。认证测试技术是一种在串空间模型基础上发展而来的一种新型的安全协议分析技术,使安全协议的分析过程更为简洁与直观。但是,目前几乎所有的形式化分析方法包括 BAN 逻辑[5]等,在协议为什么不正确方面的分析能力都显得较弱。

安全协议的正确性主要体现为一致性和机密性两个方面,本文主要在认证测试基础上,利用参数一致性矩阵讨论协议一致性方面的问题。文章第 2 节简单介绍了一些相关的基本概念和结论。第 3 节详细描述了参数一致性矩阵以及在该矩阵上的运算规则。第 4 节利用参数一致性矩阵以 Otway-Rees 协议为例进行分析,指出该协议存在缺陷的根源所在并给出了具体的改进方向。最后对本文的工作进行了简要的总结。

2　串空间模型和认证测试

对文章所涉及的串空间模型和认证测试方法中的一些基本概念和相关性质进行简单介绍,详细内容请参阅文[1,3,4]。

2.1　基本概念

定义 1　子项关系

子项关系$\sqsubset$可以递归定义为满足下列关系的最小关系:

(1)$a\sqsubset a$;

(2)$a\sqsubset\{g\}_k$,如果$a\sqsubset g$;

(3)$a\sqsubset g\neq h$,如果$a\sqsubset g\vee a\sqsubset h$。

如果$g\sqsubset h$并且$g\neq h$,那么就称 g 是 h 的一个严格子项(proper subterm)。

在有些情况下,需要应用更广的关系$\sqsubset'$

$a\sqsubset'\{g\}_k$ iff $a\sqsubset' g\vee a=k\vee a=\{g\}_k$

定义 2　原子项、加密项和级联项

(1)如果项$a\in T\cup K$,那么项 a 就是原子项。其中 T 是原子消息集合,比如人名、随机数、时间戳等;K 是密钥集合。

(2)如果项 a 具有形式$\{g\}_k$,那么项 a 就是加密项。其中$k\in K$。

(3)如果项 a 能表示成形式 gh,那么项 a 就是级联项。

定义 3　组件(component)

项 t_0 是 t 的一个组件当且仅当满足以下条件:

(1)$t_0\sqsubset t$ 且 t_0 不是级联项;

(2)对于任意$t_1\neq t_0$,如果$t_0\sqsubset t_1\sqsubset t$,那么 t_1 是级联类型的消息。

组件或者是原子消息类型或者是加密消息类型。

项 t 是节点$n=(s,i)$的新组件,当且仅当 t 是 term(n)的组件,并且不是其他节点$n=(s,j)(i>j)$的组件。

定义 4　(Transforming Edge 和 Transformed Edge)

(1)边$n_1\Rightarrow^+ n_2$是关于$a\in A$的 Transforming Edge,当且仅当 n_1 是负节点,n_2 是正节点,并且存在 n_2 的一个新组件 t_2,使得$a\sqsubset t_2$。

(2)边$n_1\Rightarrow^+ n_2$是关于$a\in A$的 Transformed Edge,当且仅当 n_1 是正节点,n_2 是负节点,并且存在 n_2 的一个新组件 t_2,使得$a\sqsubset t_2$。

定义 5　测试组件(Testing Component)

$t=\{h\}_k$是 a 在节点 n 中的一个测试组件,如果满足以下条件:

(1)$a\sqsubset t$,并且 t 是节点 n 的组件;

(2)项 t 不是串空间Σ中任意其他正则节点的组件的严

*)基金项目:国家自然科学基金(69873040)。**周清雷**　教授,CCF 高级会员,硕士生导师,主要研究方向为模型检测、安全协议分析、自动机理论;**王　峰**　硕士研究生,研究方向为安全协议分析;**赵东明**　副教授,主要研究方向为网络安全。

格子项(proper subterm)。

如果 a 唯一起源于节点 n_0,并且边 $n_0 \Rightarrow^+ n_1$ 是关于 a 的 Transformed Edge,那么我们就称边 $n_0 \Rightarrow^+ n_1$ 是 a 的一个测试。

定义 6 出测试(Outgoing Test)

边 $n_0 \Rightarrow^+ n_1$ 是项 $t=\{h\}_k$ 关于 a 的出测试,如果满足以下条件:

(1)边 $n_0 \Rightarrow^+ n_1$ 是 a 的一个测试;

(2)$k^{-1} \notin P$;

(3)a 不在节点 n_0 的除 t 以外的任何其它组件中出现;

(4)t 是节点 n_0 关于 a 的一个测试组件。

定义 7 入测试(Incoming Test)

边 $n_0 \Rightarrow^+ n_1$ 是项 $t=\{h\}_k$ 关于 a 的入测试,如果满足以下条件:

(1)边 $n_0 \Rightarrow^+ n_1$ 是 a 的一个测试;

(2)$k \notin P$;

(3)t 是节点 n_1 关于 a 的一个测试组件。

定义 8 主动测试(Unsolicited Test)

一个负节点 n 是项 $t=\{h\}_k$ 的一个主动测试,如果满足以下条件:

(1)对 n 中任意的 a 来说,t 是节点 n 关于 a 的测试组件;

(2)$k \notin P$。

2.2 认证测试的性质

认证测试 1 假设 C 是一个丛,节点 $n' \in C$,边 $n \Rightarrow^+ n'$ 是项 t 关于 a 的一个出测试,那么我们可以得到以下结论:

(1)存在正则节点 $m, m' \in \Sigma$ 使得 t 是 m 的一个组件,并且边 $m \Rightarrow^+ m'$ 是值 a 的 Transforming Edge;

(2)如果假设 a 只在节点 m 的组件 $t_1=\{h_1\}_{k_1}$ 中出现,t_1 不是任何其他正则节点组件的严格子项,并且 $k_1^{-1} \notin P$,那么必然存在一个负的正则节点 m'',使得 t_1 为 m'' 的组件。

认证测试 2 假设 C 是一个丛,节点 $n' \in C$,边 $n \Rightarrow^+ n'$ 是项 t' 关于 a 的一个入测试,那么必然存在正则节点 $m, m' \in C$ 满足 t' 是 m' 的消息组件,并且边 $m \Rightarrow^+ m'$ 是 a 的 Transforming Edge。

认证测试 3 假设 C 是一个丛,节点 $n \in C$,并且 n 是项 $t=\{h\}_k$ 的一个主动测试,那么存在一个符号为正的正则节点 $m \in C$,使得 t 是 m 的一个组件。

3 参数一致性矩阵

安全协议的正确性主要体现为一致性和机密性两个方面,这里主要讨论一致性方面的问题。需要指出的是,安全协议的一致性必须建立在协议机密性的基础上。协议对于机密性的保证相对而言要简单得多,并且大部分协议都能提供机密性的保证,这里对这方面的问题不做讨论。

3.1 一致性概念

"一致性(agreement property)"也称"对应性(correspondence property)",对某个参数向量 $\vec{X}$,称一个安全协议保证了对主体 B(响应者)的一致性是指:任何时候 B 作为响应者(B 认为他在和 A 进行会话)使用参数向量 $\vec{X}$ 完成了一轮协议;则必定存在唯一的一轮协议,在这轮协议中 A 使用相同的参数向量 $\vec{X}$ 发起了一次会话,且 A 认为他是在和 B 进行会话。

令 Resp($\vec{X}$)和 Init($\vec{X}$)分别代表使用参数 $\vec{X}$ 实例化的响应者串和发起者串,假如有一个参数是唯一地起源于串 Init($\vec{X}$),则发起者串 Init($\vec{X}$)$\in C$ 显然是唯一的,在这种情况下,就验证了协议的一致性。

3.2 参数一致性矩阵

假设在串空间 Σ 上,某个协议执行的过程中,主体 A 和 B 所对应的参数向量分别记为 $\vec{m}$ 和 $\vec{n}$,一般来说参数向量 $\vec{m}$ 和 $\vec{n}$ 是不完全相同的。由于 A 和 B 不可能在那些只出现在其中一个向量中的参数上取得"一致",因此,把向量 $\vec{m}$ 和 $\vec{n}$ 的公共参数记为向量 $\vec{t}$。显然,主体 A 和 B 认证过程中只可能在向量 $\vec{t}$ 的部分或者全部分量上达成"一致"。

对参与协议运行的主体 A 和 B 来说,它们的参数一致性矩阵 $M=(m_{ij})_{n\times n}$ 要满足下列条件:

(1)M 是一个 $n \times n$ 的矩阵。其中 $n=|\vec{t}|$,即向量 $\vec{t}$ 的维数;

(2)依次以 $\vec{t}$ 的分量表示矩阵 M 的行和列;

(3)$m_{ij}=\varnothing$,如果 $i \neq j$。$m_{ij}=(x,y)$,如果 $i=j$,其中 $\{x \mid x=0$ 或 $1\}$,$\{y \mid y \geqslant 0, y \in N\}$。

例如,对于主体 A、B 来说,如果他们的公共参数对应的向量为 $\vec{t}=(p,q,r)$,那么它们的参数一致性矩阵就可表示为:

$$M=\begin{bmatrix}(x_1,y_1) & \varnothing & \varnothing \\ \varnothing & (x_2,y_2) & \varnothing \\ \varnothing & \varnothing & (x_3,y_3)\end{bmatrix}$$

3.3 参数一致性矩阵的解释

以上面的矩阵 M 为例,由主体 A 和 B 的公共参数生成的向量为 $\vec{t}=(p,q,r)$。

(1)矩阵中元素为 $m_{ij}=(x,y)$ 的位置,表示主体 A 和 B 在该位置对应的参数在认证的过程中可能会取得一致。显然,这样的元素只可能在 $i=j$ 的位置上。如果在认证的过程中在该参数上取得一致则 $x=1$,y 的值是认证过程中相应参数取得一致性时的串的高度。

(2)元素为$\varnothing$的位置表示 A 和 B 在该位置对应的参数,在认证的过程中不能取得一致。显然,元素 $m_{ij}=\varnothing (i \neq j)$;在 $i=j$ 的位置上,如果认证过程中在该参数上没有取得一致,则该处元素也记为$\varnothing$。

3.4 参数一致性矩阵的运算规则

设 $A=(a_{ik})_{n\times n}$,$B=(b_{kj})_{n\times n}$ 为两个参数一致性矩阵,矩阵 $C=(c_{ij})_{n\times n}$ 是 A 与 B 的乘积,其中:

(1)矩阵的运算规则与一般的矩阵运算规则相同,即 $c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{is}b_{sj}=\sum_{k=1}^{s}a_{ik}b_{kj}$ 其中,$(i=1,2,\cdots,n; j=1,2,\cdots,n)$。

(2)矩阵中元素间的运算满足规则:(i)如果 $a=\varnothing$ 或者 $b=\varnothing$,那么 $ab=\varnothing$;如果 $a=(x_1,y_1)$,$b=(x_2,y_2)$,那么 $ab=(x,y)$。其中,$x=x_1 \wedge x_2$,即做逻辑与运算;$y=y_2$。(ii)如果 $a=\varnothing, b \neq \varnothing$,那么 $a+b=b$;如果 $a=\varnothing, b=\varnothing$,那么 $a+b=a$;如果 $a=\varnothing, b=\varnothing$,那么 $a+b=\varnothing$。

4 协议分析

下面以 Otway-Rees 协议为例,来说明参数一致性矩阵在安全协议一致性分析方面的应用。

4.1 Otway-Rees 协议

Otway-Rees 协议是一个密钥分发协议,具体如下:

(1)$A \rightarrow B: M, A, B, \{N_a, M, A, B\}_{Kas}$

(2)$B \rightarrow S: M, A, B\{N_a, M, A, B\}_{Kas}, \{N_b, M, A, B\}_{Kbs}$

(3)$S \rightarrow B: M, \{N_a, K_{ab}\}_{Kas}, \{N_b, K_{ab}\}_{Kbs}$

(4)$B \rightarrow A: M, \{N_a, K_{ab}\}_{Kas}$

协议有三个参与者:发起者(A)、响应者(B)和认证服务器(S)。协议的目的是密钥分配服务器 S 为主体 A,B 生成并分发一个会话密钥。如图 1 所示,其中 M 是协议回合的标识符。

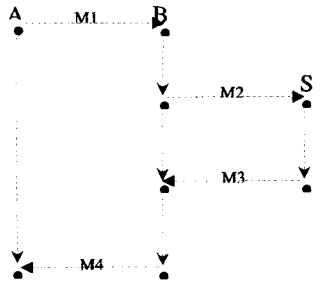

图 1　Otway-Rees 协议的 Strand 结构图

$M1=MAB\{N_aMAB\}_{Kas}$

$M2=MAB\{N_aMAB\}_{Kas}\{N_bMAB\}_{Kbs}$

$M3=M\{N_aK_{ab}\}_{Kas}\{N_b,K_{ab}\}_{Kbs}$

$M4=M\{N_aK_{ab}\}_{Kas}$

4.2　Otway-Rees 协议的一致性分析

Otway-Rees 协议中的正则串定义为如下形式：

(1)发起者串 $s\in \mathrm{Init}[A,B,N_a,M,K]$，与它对应的迹为

$\langle +MAB\{N_aMAB\}_{\mathrm{Kas}},-M\{N_aK\}_{\mathrm{Kab}}\rangle$

$\mathrm{Init}[A,B,N_a,M,K]$表示了所有具有上述迹的串集合，与这种串对应的活动主体是 A。

(2)响应者串 $s\in \mathrm{Resp}[A,B,N_b,M,K,H,H']$，与它对应的迹为

$\langle -MABH,+MABH\{N_bMAB\}_{Kbs},-MH'\{N_bK\}_{Kbs},+MH'\rangle$

$\mathrm{Resp}[A,B,N_b,M,K,H,H']$表示了所有具有上述迹的串的集合，与这种串对应的活动主体是 B。

(3)服务器串 $s\in \mathrm{Serv}[A,B,N_a,N_b,M,K]$，与它对应的迹为

$\langle -MAB\{N_aMAB\}_{Kas}\{N_bMAB\}_{Kbs},+M\{N_aK\}_{Kas}\{N_bK\}_{Kbs}\rangle$

$\mathrm{Serv}[A,B,N_a,N_b,M,K]$表示了所有具有上述迹的串的集合，与这种串对应的活动主体是某一个固定的服务器 S_0。

发起者 A 对应的参数向量记为 $\vec{t}_A=(A,B,N_a,M,K)$，响应者 B 对应的参数向量记为 $\vec{t}_S=(A,B,N_b,M,K,H,H')$，服务器 S 对应的参数向量记为 $\vec{t}_S=(A,B,N_a,N_b,M,K)$。

服务器的保证

设 C 为丛，$K_{as},K_{bs}\notin K_p$；$A\neq B$；$s_s\in \mathrm{Serv}[A,B,N_a,N_b,M,K]$的 C-height=2。由 $\vec{t}_A$ 和 $\vec{t}_S$ 的公共参数生成的向量为(A,B,Na,M,K)，由 $\vec{t}_B$ 和 $\vec{t}_S$ 的公共参数生成的向量为(A,B,N_b,M,K)。项$\{N_aMAB\}_{Kas}$和项$\{N_bMAB\}_{Kbs}$都是节点$\langle s_s,1\rangle$的主动测试，由认证测试 3 可得 S 和 A 以及 S 和 B 的参数一致性矩阵分别为：

$$M_{SA}=\begin{bmatrix}(1,1)&\varnothing&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,1)&\varnothing&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,1)&\varnothing&\varnothing\\ \varnothing&\varnothing&\varnothing&(1,1)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing&\varnothing\end{bmatrix}$$

$$M_{SB}=\begin{bmatrix}(1,2)&\varnothing&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,2)&\varnothing&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,2)&\varnothing&\varnothing\\ \varnothing&\varnothing&\varnothing&(1,2)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing&\varnothing\end{bmatrix}$$

也就是说，在丛 C 中，如果有 $s_s\in \mathrm{Serv}[A,B,N_a,N_b,M,K]$，那么存在发起者串 $s_i\in \mathrm{Init}[A,B,N_a,M,*]$和响应者串 $s_r\in \mathrm{Resp}[A,B,N_b,M,*,*,*]$，且 s_i 的 C-height=1，s_r 的 C-height=2。

在文[6]中对认证参数提供了更为详细的分类。

发起者的保证

设 C 为丛，$K_{as}\notin K_p$；$A\neq B$；$s_i\in \mathrm{Init}[A,B,N_a,M,K]$的 C-height=2。由 $\vec{t}_A$ 和 $\vec{t}_S$ 的公共参数生成的向量为(A,B,N_a,M,K)。边$\langle s_i,1\rangle\Rightarrow^+\langle s_i,2\rangle$是项$\{N_aMAB\}_{Kas}$关于 N_a 的一个出测试，同时它还是项$\{N_aK\}_{Kas}$关于 N_a 的一个入测试，由认证测试 1 和认证测试 2 可得 A 和 S 的参数一致性矩阵为：

$$M_{AS}=\begin{bmatrix}(1,2)&\varnothing&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,2)&\varnothing&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,2)&\varnothing&\varnothing\\ \varnothing&\varnothing&\varnothing&(1,2)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing&(1,2)\end{bmatrix}$$

也就是说，在丛 C 中，如果有 $s_i\in \mathrm{Init}[A,B,N_a,M,K]$，那么存在服务器串 $s_s\in \mathrm{Serv}[A,B,N_a,*,M,K]$，且 s_s 的 C-height=2。

在这里对于发起者 A 来说，不能够直接得到 A 和 B 的参数一致性矩阵 M_{AB}，是因为在 A，B 两个主体之间不存在以上三种类型的认证测试，后面我们将讨论如何得到 M_{AB}。

响应者的保证

设 C 为丛，$K_{bs}\notin K_p$；$A\neq B$；$s_r\in \mathrm{Init}[A,B,N_b,M,K]$的 C-height=3。由 $\vec{t}_B$ 和 $\vec{t}_S$ 的公共参数生成的向量为(A,B,N_b,M,K)。边$\langle s_r,2\rangle\Rightarrow^+\langle s_r,3\rangle$是项$\{N_bMAB\}_{Kbs}$关于 N_b 的一个出测试，同时它还是项$\{N_bK\}_{Kbs}$关于 N_b 的一个入测试，由认证测试 1 和认证测试 2 可得 B 和 S 的参数一致性矩阵为：

$$M_{BS}=\begin{bmatrix}(1,2)&\varnothing&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,2)&\varnothing&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,2)&\varnothing&\varnothing\\ \varnothing&\varnothing&\varnothing&(1,2)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing&(1,2)\end{bmatrix}$$

也就是说，在丛 C 中，如果有 $s_r\in \mathrm{Resp}[A,B,N_b,M,K,H,H']$，那么存在服务器串 $s_s\in \mathrm{Serv}[A,B,*,N_b,M,K]$，且 s_s 的 C-height=2。

同样，对于响应者 B 来说，也不能够直接得到 B 和 A 的参数一致性矩阵 M_{BA}。

如果 $s_i\in \mathrm{Init}[A,B,N_a,M,K]$在丛 C 中，由发起者的保证可知，存在 $s'\in \mathrm{Serv}[A,B,N_a,*,M,K]$也在该丛中，进一步由服务器的保证可知，在丛 C 中存在某个 $s_r\in \mathrm{Resp}$。这样就可以得到响应者 B 对发起者 A 的保证，即 A 和 B 的参数一致性矩阵 M_{AB}。用矩阵的乘法来表示这种间接的认证过程。在计算 M_{AB} 之前先要对矩阵 M_{AS} 和 M_{SB} 进行简单处理，保留 M_{AS} 和 M_{SB} 中公共参数(A,B,M,K)对应的行和列，得到两个新的矩阵 M'_{AS} 和 M'_{SB}，依照前面提供的运算规则可得，$M_{AB}=M'_{AS}M'_{SB}$ 即：

$$M_{AB}=M'_{AS}M'_{SB}=\begin{bmatrix}(1,2)&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,2)&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,2)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing\end{bmatrix}$$

也就是说，在丛 C 中，如果 $s_i\in \mathrm{Init}[A,B,N_a,M,K]$，那么存在响应者串 $s_r\in \mathrm{Resp}[A,B,*,M,*]$，且 s_r 的 C-height=2。

同理，$M_{BA}=\begin{bmatrix}(1,1)&\varnothing&\varnothing&\varnothing\\ \varnothing&(1,1)&\varnothing&\varnothing\\ \varnothing&\varnothing&(1,1)&\varnothing\\ \varnothing&\varnothing&\varnothing&\varnothing\end{bmatrix}$。即在丛 C 中，如果 $s_r\in \mathrm{Resp}[A,B,N_b,M,K,H,H']$，那么存在 $s_i\in \mathrm{Init}[A,B,*,M,*]$，且 s_i 的 C-height=1。

4.3 结果分析

由矩阵 M_{AB} 可以看出，Otway-Rees 协议中主体 A 和 B 并没有对 S 分配的会话密钥 K 达成一致，从而导致了协议的失败。为什么会出现这样的结果呢？通过参数一致性矩阵 M_{AB} 的生成过程可以得到说明，由 M_{AS} 可知主体 A 和 S 在密钥 K 上达成一致，也就是说 A 能够确认 K 是 S 为 A 和 B 分配的会话密钥；而由 M_{SB} 可知主体 S 和 B 并没有在密钥 K 上取得一致，也就是说 S 不能确认 B 是否收到了会话密钥 K，正因如此，才使得主体 A 和 B 对 K 不能达成一致造成协议失败。

通过对协议失败原因的分析，为我们提供了两种改进协议的思路：(1)使主体 B 和 S 在参数 K 上也能够达成一致；(2)在 A 和 B 之间提供直接的认证测试组件，使主体 A 和 B 在密钥 K 和其他关键参数上直接达成一致。

总结 认证测试技术的出现，使安全协议的分析过程变得更为简捷与直观。本文使用认证测试技术结合参数一致性矩阵，对安全协议的一致性进行了更为深入的分析，从而揭示了协议失败的原因，并针对这些原因给出相应改进的思路。对那些在协议中没有直接提供认证测试的主体来说，通过矩阵运算的方法实现间接认证，由于过程更为形式化使得对协议的分析更容易实现自动化。

参 考 文 献

1 Guttman JD, Fàbrega FJT. Authentication tests and the structure of bundles. Theoretical Computer Science, 2002, 283(2): 333～380

2 Guttman JD. Security protocol design via authentication tests. In: Proc. of the 2002 IEEE Computer Society Foundations Workshop. Los Alamitos: IEEE Computer Society Press, 2002. 92～103

3 Thayer FJ, Herzog JC, Guttman JD. Strand spaces: Why is a security protocol correct[A]? In: Proceedings of the 1998 IEEE Symposium on Security and Privacy[C]. Los Alamitos: IEEE Computer Society Press, 1998. 160～171

4 Thayer FJ, Herzog JC, Guttman JD. Honest ideals on strand spaces[A]. In: Proceedings of the 1998 IEEE Computer Security Foundations Workshop[C]. Los Alamitos: IEEE Computer Society Press, 1998. 66～77

5 Burrows M, Abadi M, Needham R. A logic of Authentication[J]. ACM Transactions on Computer systems, 1990(8): 18～36

6 YANG Ming, LUO Jun-Zhou. Analusis of Security rotocols Based on Authentication Test. Journal of Software, 2006, 17(1): 148～156

(上接第 87 页)

进一步降低污染 WAPI IE 造成的危害。

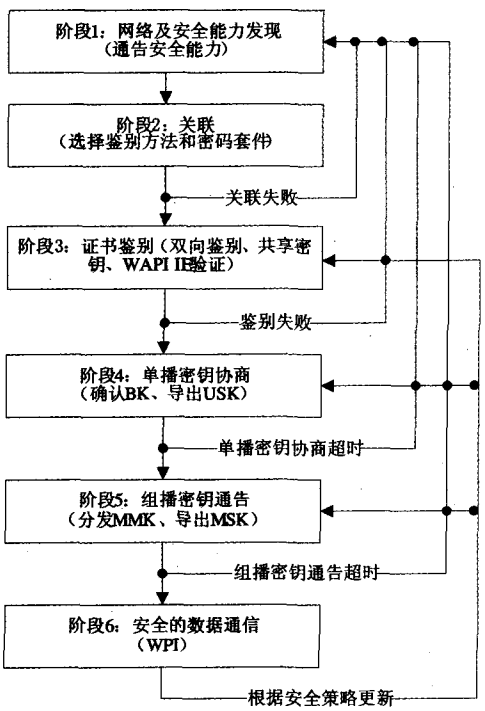

图 4 WAPI 的可用性实施方案

(4)采用合适的失败恢复方案提高整个协议的效率。在低速移动的无线网络中，若证书鉴别已成功完成，则协议失败应从最近处恢复；反之，将从头开始恢复。在高速移动的无线网络中，则协议失败从头恢复较好。因此，改进后的协议失败恢复点要比原始方案多出一些。

(5)为了提高安全性，尽可能对管理帧进行鉴别。一旦成功完成了鉴别过程，导出的共享基密钥可用于鉴别后续的管理帧，特别是 Deauthentication 和 Disassociation。这种方法可避免对多数管理帧的攻击，除 WAPISA 建立之前的管理帧由于共享密钥尚未得到而未被鉴别外。

(6)AE 和 ASUE 端口打开后，WAPI 协议数据以明文方式传输。在 IEEE 802.11i 中，4 步握手完成后，IEEE 802.1x 鉴别与密钥管理协议数据以密文形式传输，即受 WEP、TKIP 或者 CCMP 的保护。当 ASUE 收到消息 3 发出消息 4 后，将受控端口打开(Unblocked)，而 AE 由于无线丢包的原因未收到消息 4，则 AE 端的受控端口的状态仍为关闭(Blocked)。此时 AE 超时重传明文的消息 3 时，ASUE 端因只能接受加密的协议数据而收不到消息 3，从而造成此次 4 步握手协议失败。众所周知，无线的丢包率较高，那么 4 步握手协议的失败率也就不言而喻，这是 IEEE 802.11i 中 4 步握手协议存在的一大瑕疵。为了避免这种现象，在 WAPISA 中，AE 和 ASUE 的端口不论是否打开，WAPI 协议数据均以明文传输。

通过上述措施，WAPI 改进方案可避免有可能遭受的脆弱性，使得协议更加实用，提高执行效率。

结束语 WAPI 是为了解决无线局域网国际标准中的安全漏洞而设计的安全增强协议，主要保护无线网络中数据传输的机密性、完整性、鉴别性，同时对请求接入网络的用户进行身份鉴别和访问控制，保障合法的用户安全接入并安全访问合法的网络。笔者从协议的可用性角度分析了管理帧面临的各种攻击，并定义了一些防范措施，为 WAPI 协议的更好实施提供建议。但由于无线串路的脆弱性，DoS 攻击总能通过频率阻塞、网络阻塞及其他手段存在，因此这里给出的 WAPI 可用方案能有效地防御串路层的 DoS 攻击，并不能避免所有脆弱性。

参 考 文 献

1 黄振海，郭宏，王育民，等. GB15629.11-2003/XG1-2006《信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分：无线局域网媒体访问控制和物理层规范》. 中国标准出版社，2003

2 赖晓龙，曹军，铁满霞，等. GB15629.11-2003/XG1-2006《信息技术系统间远程通信和信息交换局域网和城域网特定要求第 11 部分：无线局域网媒体访问控制和物理层规范第 1 号修改单》. 中国标准出版社，2006

3 He Changhua, Mitchell J C. Security Analysis and Improvements for IEEE 802.11i. In: Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS05), 2005

4 Canetti R, Krawczyk H. Analysis of Key exchange Protocol and Their Use for Building Secure Channels[A]. In: Proceeding of Eurocrypt 2001: LNCS 2 045[C]. Berlin: Springer 2 Verlag, 2001. 453～474

5 AusCERT AA-2004.02. Denial of Service vulnerability in IEEE 802.11 wireless devices. May 13, 2004. http://www.auscert.org.au/render.html?it=4091

6 IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements. ANSI/IEEE Std 802.11i, 2004-6-24

7 IEEE Computer Society LAN MAN Standards Committee. Port-based Network Access Control. ANSI/IEEE Std 802.1x, 2004-11-15