TLS 协议认证测试模型与形式化分析

孔 娟,曹利培
KONG Juan,CAO Li-pei

安阳工学院 计算机科学与信息工程系,河南 安阳 455000
Department of Computer Engineering,Anyang Institute Technology,Anyang,Henan 455000,China
E-mail:kongjuan2000@yahoo.cn

KONG Juan,CAO Li-pei.Formalized analysis for authentication test model of TLS.Computer Engineering and Applications, 2009,45(23):100-103.

Abstract: TLS protocol is an important transport layer security protocol,and is widely used.Based on strand space theory,this paper points out the DH parameter signature certification testing program,analyzes and proves the confidentiality and authentication of the agreement.The result shows that the TLS protocol meets their security statement.
Key words: Transport Layer Security(TLS) protocol;authentication test;strand space;formalized analysis

摘 要:TLS 协议是一种重要的传输层安全协议,得到了广泛的应用。在结合串空间理论和方法的基础上,通过构造 TLS 握手协议的认证测试模型,提出了 TLS 协议的 DH 参数签名认证测试方案,分析和证明了协议的保密性和认证性等关键属性。结果表明 TLS 协议满足其安全性说明。
关键词:传输层安全协议;认证测试;串空间;形式化分析
DOI:10.3778/j.issn.1002-8331.2009.23.028 **文章编号:**1002-8331(2009)23-0100-04 **文献标识码:**A **中图分类号:**TP393

传输层安全(Transport Layer Security,TLS)协议是 IETF于 1999 年正式发布的基于传输层的安全协议草案(RFC 2246)[1],该协议基于 Netscape 公司的安全套接字层 (Secure Socket Layer,SSL)协议 3.0 版本。从发布以来,TLS 协议在互联网上已得到广泛应用, 除了如 S/HTTP,S/MIME,SSL-Telnet,SSL-SMTP,SSL-POP3 等常用协议外, 在电子商务和电子政务系统中也大量采用, 其重要性不容置疑。经过不断更新,IETF 于 2008 年 8 月发布了 TLS 的最新版本——TLS Version 1.2(RFC 5246)[2]。

认证测试[3-4]思想是串空间理论[5]的又一重要成果,通过构造协议认证测试(Authentication Test)模型来形式化地描述和分析协议的认证属性,因其直观、简洁、能清晰描述协议认证过程的优点,得到广泛应用[3-4,6-9]。

通过构造 TLS 协议 1.2 版[2]的认证测试模型,分析和证明协议的保密性和认证性等关键属性,结果表明 TLS 协议满足其安全性说明[2]。

1 相关研究

TLS 协议自发布以来,众多学者对其进行了分析研究。主要成果有:Paulson 采用归纳法对 TLS 进行了形式化分析[10];Calixto 和 Monroy 使用 CADP 方法分析了 TLS 协议的安全性[11];Ogata 和 Futatsugi 采用方程式的方法分析了 TLS 的分布式属性[12];孙林红等人结合 PKI 的研究成果对 TLS 协议进行了修改[13];倪阳和张玉清采用随机预言机方法分析了 TLS 协议的计算模型[14]。另外,Jonathan C.Herzog 采用串空间理论建立了简化 TLS 协议的 Diffie-Hellman 密钥协商机制,并分析了该密钥协商机制的安全性[15]。

这些工作都是针对 TLS 协议 1.0 版本的分析和研究,该文则在 Jonathan C.Herzog 的研究工作基础上,结合认证测试的思想对 TLS 协议 1.2 版本进行分析,建立其认证测试模型,分析和证明它的保密性和认证性等关键属性。

2 TLS 协议

TLS 协议是一种独立的传输层安全协议,可以保持对上层协议的透明性。TLS 协议的主要目标是为两个通信实体之间提供数据的保密性和完整性,进行实体间的身份认证。协议分为两层:TLS 记录协议和 TLS 握手协议, 下面简要介绍 TLS 记录协议和 TLS 握手协议[2]。

2.1 TLS 记录协议

TLS 记录协议的一条记录包含长度域、描述域和内容域。记录协议得到要发送的消息之后, 将数据分成易理的数据分组,进行数据压缩处理,计算数据分组的密码校验值 MAC,加密数据,然后发送数据。接收消息首先被解密,然后校验 MAC,解压缩,重组,最后传递给协议的高层客户。记录协议有 4 种类型的客户:握手(handshake)协议、警告(alert)协议、改变密码规格(change cipher spec)协议和应用数据(application data)协

作者简介:孔娟(1966-),女,副教授,研究领域为:多媒体信息处理、网络信息安全;曹利培,讲师,研究领域为:SOA、Web 服务、形式化和语义等。
收稿日期:2009-03-23 **修回日期:**2009-05-26

议。便于 TLS 协议的扩展,记录协议可以支持额外的记录类型。

2.2　TLS 握手协议

TLS 握手协议建立连接会话,协商新建会话的密码学参数,该过程在 TLS 记录协议之上进行。当 TLS 协议的客户和服务器开始第 1 次通信时,首先需要协商协议版本,选择密码算法,相互进行认证,并使用公钥密码技术生成共享秘密。如果客户和服务器希望恢复已有会话,那么可选择进行简化版的握手协议。该文工作主要针对完整的 TLS 握手协议,包括以下步骤:

(1)交换 Hello 消息以协商密码算法,交换随机值并检查会话是否可重用。

(2)交换必要的密码学参数,使客户和服务器能够协商预主密钥(premaster secret)。

(3)交换证书和密码学信息,使客户和服务器能够进行相互认证。

(4)使用交换的随机值和预主密钥生成主秘密(master secret)。

(5)为记录协议提供安全参数。

(6)允许客户和服务器验证它与通信对端计算了相同的安全参数,并验证当前已经完成的握手过程不存在攻击者的干预。

TLS 握手协议提供了三种认证和密钥协商方法:一是匿名的密钥协商;二是 RSA 密钥协商和认证;三是 Diffie-Hellman 密钥协商和认证。该文工作主要针对第三种认证和密钥协商方法,为便于分析,提取握手协议运行流程,并进行初步形式化抽象。C 表示客户端,S 表示服务器,协议描述如下:

$C\rightarrow S:R_c$;

$S\rightarrow C:R_s,SID,CertS,Y_s,[|R_c,R_s,Y_s|]_{Ks}$;

$C\rightarrow S:CertC,Y_c,CertVer_c,F_c$;

$S\rightarrow C:F_s$;

其中,R_a 表示由实体 A 产生的任意随机值;SID 表示由服务器分配的当前会话的标志符;CertA 表示实体 A 拥有的签名公钥证书,证书格式参考 X.509 协议标准[16];Y_a 表示实体 A 产生的临时 Diffie- Hellman 公共秘密参数,$Y_a=g^x \bmod p$;$[|R_c,R_s,Y_s|]_{Ks}$ 表示服务器对连接消息(R_c,R_s,Y_s)的签名;$CertVer_c=[|R_c,R_s,SID,CertS,CertC,Y_s,Y_c,[|R_c,R_s,Y_s|]_{Ks}|]_{Kc}$ 表示证书验证消息;F_a 表示握手协议结束,其消息格式为 PRF(SK,hash(handshake_messages)),这里,PRF 为伪随机函数(Pseudorandom function),SK 是计算出的当前会话主密钥,"handshake_messages" 表示当前握手协议所传输的所有消息,包括 $\{|R_c,R_s,SID,CertS,CertC,Y_s,Y_c,[|R_c,R_s,Y_s|]_{Ks},CertVerc,F_c|\}$,但是,为了区分,$F_c$ 并不包含自身,而 F_s 则含有 F_c。主密钥 SK 由下式计算:

$SK=PRF(pre\_master\_secret,R_c+R_s)$

其中,"pre_master_secret"为双方交换的 Diffie-Hellman 密钥。

3　串空间基本概念与理论

本章简要介绍串空间基本理论和认证测试模型,完整内容请参考文献[3-5]。

3.1　串空间基本概念

串空间理论[5]是由 Fabrega,Herzog 和 Guttman 提出的一种安全协议形式化分析方法,结合定理证明和协议迹思想,借助带有因果关系的有向图来描述协议的执行过程。串空间模型能准确地描述协议执行过程中事件的先后顺序及因果关系,为研究人员提供了一种有效的协议分析理论。

串(Strand)指的是一轮协议运行到某个时刻某个实体所发生的行为事件的一个消息序列,由发送和接收的消息序列组成。串空间(Strand Space)是某个协议的运行当中所有可能出现的串的集合,包括所有的协议合法实体的串和所有攻击者的串,用 Σ 表示。不同协议实体的串之间通过消息数据的收发相互关联从而形成丛(bundle)。集合{+,-}是串空间的动作集,其中"+"表示发送消息,"-"表示接收消息。节点(node)是一个二元组 $n=<s,i>$,其中,$s\in\Sigma$ 表示串空间中的一个串,i 是一个大于 0 的整数,表示节点 n 在串中的序号,节点集合记为 N。对于 $n_1,n_2\in N$,存在一条边 $n_1\rightarrow n_2$,当且仅当 $term(n_1)=+a$,且 $term(n_2)=-a$,其中 $term(n)$表示节点 n 的消息项,a 表示信道上传输的消息。这类边表示在节点 n_1 发送消息 a,并在节点 n_2 接收消息 a,它记录了串间的一种因果连接。如果 $n_1=<s,i>\in N$,$n_2=<s,i+1>\in N$,则存在边 $n_1\Rightarrow n_2$,这类边表示 n_1 是 n_2 在串 s 上的直接因果前驱。用 $n'\Rightarrow^{+}n$ 表示 n' 是 n 在同一个串上的因果前驱(不一定是直接因果前驱)。

3.2　Diffie-Hellman 机制的串空间扩展

为 Diffie-Hellman 密钥交换机制增加类型 D,用 $d_1,d_2,\cdots$ 表示 D 的成员,$d=g^x$,定义操作:

DH:$D\times D\rightarrow D$

描述 Diffie-Hellman 密钥交换机制,则 $DH(d_1,d_2)=g^{xy}$。

定义 1　消息项集合 A 由以下无关集合组成:

(1)$T\subset A$,T 由可预知消息组成;

(2)$R\subset A$,R 由不可预知的随机值组成;

(3)$K\subset A$,K 为密钥集;

(4)$D\subset A$,D 包含 Diffie-Hellman 值。

密钥集合 K 分为下面四个无关集:

(1)签名密钥集,用 K_{Sig} 表示;

(2)签名验证密钥集,用 K_{Ver} 表示;

(3)对称密钥集,用 K_{Sym} 表示;

(4)入侵者密钥集,用 K_P 表示。

消息项运算由下面五种操作组成:

(1)hash:$A\rightarrow A$,描述散列运算;

(2)encr:$K_{Sym}\times A\rightarrow A$,描述加密运算;

(3)sig:$K_{Sig}\times A\rightarrow A$,描述签名运算;

(4)jion:$A\times A\rightarrow A$,描述两个消息项的级联;

(5)DH:$D\times D\rightarrow D$,描述 Diffie-Hellman 密钥运算。

更加形式化的表达:$encr(K,M)=\{|M|\}_K$,而 $sig(K,M)=[|M|]_K$。更详细的描述请参考文献[15]。

3.3　认证测试理论

Guttman 等人提出的认证测试理论[3-4]通过构造协议认证测试过程模型来形式化地描述和分析协议的认证属性。

定义 2(Components)　对于项 t_0、t_1 和 t,如果 $t_0\subset t$、t_0 不是级连项(concatenated),且每一个满足 $t_0\subset t_1\subset t$ 以及 $t_1\neq t_0$ 的 t_1 是一个级连项,那么称 t_0 是 t 的一个元素。

定义 3(New component)　在结点 $n=<s,i>\in N$ 中,如果项 t

是 $term(n)$的一个元素,但 t 不是任何一个在结点 n 之前出现的结点$<s,j>(j<i)$的元素,那么项 t 就是在节点 n 中出现的一个新元素。

定义 4 (Penetrable keys) 令 K_0为入侵者已知的初始密钥集,与具体某一协议无关。可入侵密钥集 K_P通过以下递归计算得出:设 $K_{P0}=K_0$,对于 $K\in Y$,$K_{Pi+1}=K_{Pi}\cup Y$,当且仅当存在一个符号为"+"的正规节点 $n\in\Sigma$,其消息项 $t\in term(n)$是 n 的一个新元素,则可入侵密钥集 $K_P=\cup_i K_{Pi}$。

由定义知,入侵者的所有密钥,要么是 K_P中已知的,要么是因为协议的合法实体将密钥置于一个新元素中而未加密保护, 要么是因为入侵者可以得到解密此新元素的解密密钥,从而得到置于新元素中的密钥。

定义 5(Safe keys) 令 K_{S0}是密钥 K 的集合,满足 $K\notin K_P$,且不存在符号为"+" 的正规结点 $n\in\Sigma$ 的新元素 t 使得 $K\subset t$。令 K_{Si+1}是密钥 K 的集合,满足 $K\notin K_P$,且对于每个符号为"+"的正规结点 $n\in\Sigma$ 以及 n 的新元素 t, 在 t 中每次出现 K 时都采用密钥 K_0进行加密,这里,$K_0^{-1}\in K_{Si}$,则安全密钥集 $K_S=\cup_i K_{Si}$。

由定义知,安全密钥集 K_S与可入侵密钥集 K_P不相交。

定义 6(Transformed edge) 对于消息 a,如果串 s 上有符号为"+"的节点 n_1和符号为"-"的节点 n_2,$a\subset term(n_1)$,且 n_2中存在一个新元素 t_2满足 $a\subset t_2$,则称 $n_1\Rightarrow^{+}n_2$是一条被转换边。

定义 7(Transforming edge) 对于消息 a,如果串 s 上有符号为"-"的节点 n_1和符号为"+"的节点 n_2,$a\subset term(n_1)$,且 n_2中存在一个新元素 t_2满足 $a\subset t_2$,则称 $n_1\Rightarrow^{+}n_2$是一条转换边。

后面,在构建 TLS 协议的认证测试模型时将重新定义测试(Test)等概念。其他相关概念参见文献[3-4]。

4 TLS 握手协议认证测试模型

接下来,通过构建 TLS 握手协议的认证测试模型来分析其认证性。下面扩展认证测试模型。

4.1 认证测试扩展

首先,重新定义测试概念。

定义 8(Test) 如果消息项 a 唯一起源(originates)于 n_0,且 $n_0\Rightarrow^{+}n_1$是 a 的一条被转换边,那么 $n_0\Rightarrow^{+}n_1$是对 a 的一个测试。称 a 为测试元素(Test component)。

TLS 握手协议的认证过程分为两步:第一步为 Diffie-Hellman 密钥协商参数的认证测试;第二步为主密钥确认。第一步的目的是为了获得新鲜的 Diffie-Hellman 公钥参数,并确保该参数来源于一个正规节点。因此,提出 DH 参数签名认证测试定理。

定义 9 (DH 参数签名测试) 令 a 是唯一起源于 n_0的测试元素,假设存在一个消息项 $t_1\subset term(n_1)$,使得新元素$[|a,d|]_K\in t_1$,这里 $K^{-1}\notin K_P$且边 $n_0\Rightarrow^{+}n_1$是对 a 的一个测试,那么,$n_0\Rightarrow^{+}n_1$是对 DH 参数的签名测试。

DH 参数签名测试串空间表示如图 1 所示。

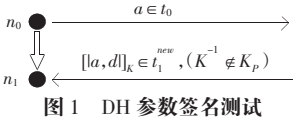


图 1 DH 参数签名测试

定理 1 (DH 参数签名认证测试) 令$\mathcal{C}$是一个丛,$\{n_0,n_1\}\subset\mathcal{C}$,且 $n_0\Rightarrow^{+}n_1$为 a 的一个 DH 参数签名测试,那么必然存在正规节点$\{m_0,m_1\}\subset\mathcal{C}$使得满足$[|a,d|]_K\in t$ 的 t 是 m_1的一个元素,且对于 a 来说,$m_0\Rightarrow^{+}m_1$是一条转换边。

DH 参数签名认证测试串空间表示如图 2 所示。

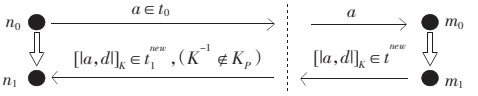


图 2 DH 参数签名认证测试

证明 假设不存在正规节点$\{m_0,m_1\}\subset\mathcal{C}$使得满足$[|a,d|]_K\in t$ 的 t 是 m_1的一个元素,那么必然存在一个符号为"+"的攻击者节点 $p\in\mathcal{C}$使得满足$[|a,d|]_K\in t'$的 t'是 p 的一个新元素。考察所有可能的入侵者串[5,15]:

M. 入侵者串为:$<+t>$,这里 $t\in T$,但是 $t'\notin T$;

R. 入侵者串为:$<+r>$,这里 $r\in R_{Adv}$,但是 $t'\notin R_P$;

C. 入侵者串为:$<-g,-h,+gh>$,此时,要么 $t'\subset g$,要么 $t'\subset h$,但是这与 t'是节点 p 的新元素矛盾;

S. 入侵者串为:$<-gh,+g,+h>$,此时与 C.串类似;

K. 入侵者串为:$<+K>$,但是 $t'\notin K_P$且 $K^{-1}\notin K_P$;

E. 入侵者串为:$<-K,-h,+\{|h|\}_K>$,但是 $t'\notin K_{Sym}$,且 $K^{-1}\notin K_P$,如果 $t'\subset h$,那么这与 t'是节点 p 的新元素矛盾;

D. 入侵者串为:$<-K,-\{|h|\}_K,+h>$,但是 $t'\notin K_{Sym}$,且 $K^{-1}\notin K_P$,如果 $t'\subset h$,那么这与 t'是节点 p 的新元素矛盾;

σ. 入侵者串为:$<-K,-h,+[|h|]_K>$,但是 $t'\notin K_{Sig}$,且 $K^{-1}\notin K_P$,如果 $t'\subset h$,那么这与 t'是节点 p 的新元素矛盾;

X. 入侵者串为:$<-[h]_K,+h>$,此时与 t'是节点 p 的新元素矛盾;

H. 入侵者串为:$<-g,+hash(g)>$,如果 $t'\subset g$,这与 t'是节点 p 的新元素矛盾;

F. 入侵者串为:$<+d>$,这里 $d\in D_p$,但是 $t'\notin D_P$。

可见,所有可能的入侵者串都不成立,因此,假设不成立。那么必然存在正规节点$\{m_0,m_1\}\subset\mathcal{C}$使得满足$[|a,d|]_K\in t$ 的 t 是 m_1的一个元素。又因为,不存在先于 m_1的节点 $m'\in\mathcal{C}$,使得 $t'\subset term(m')$满足$[|a,d|]_K\in t'$,所以 t 是 m_1的一个新元素,则对于 a 来说,$m_0\Rightarrow^{+}m_1$是一条转换边。得证。

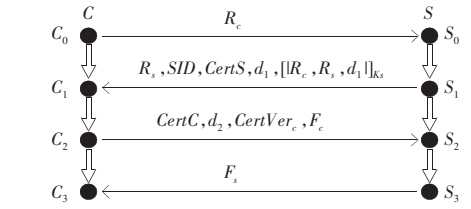
DH 参数签名认证测试表明 Diffie-Hellman 密钥协商参数"d"来自于正规的合法实体且是新鲜的,其新鲜性由测试元素"a"保证,因为发起认证测试的实体必须产生新鲜的测试元素,并验证其有效性。

4.2 TLS 握手协议认证性分析

TLS 握手协议串空间表示如图 3 所示。

首先,分析客户端和服务器的相互认证。

命题 1 令$\mathcal{C}$是包含 TLS 握手协议的丛,R_c为客户端对服务器的测试元素,节点$\{C_0,C_1\}\subset\mathcal{C}$,且 $C_0\Rightarrow^{+}C_1$为 R_c 的一个 DH 参数签名测试,则必然存在正规的服务器节点$\{S_0,S_1\}\subset\mathcal{C}$使得满足$[|R_c,*,d_1|]_{Ks}\in t$ 的 t 是 S_1的一个元素,且对于 R_c来说,



$CertVer_c=[|R_c, R_s, SID, CertS, CertC, d_1, d_2, [|R_c, R_s, d_1|]_{Ks}|]_{Kc}$

$SK=PRF(DH, R_c+R_s)$　$F=PRF(SK, hash(handshake\_messages))$

图 3　TLS 握手协议串空间

$S_0 \Rightarrow^{+} S_1$ 是一条转换边。

命题 2　令$\mathcal{E}$是包含 TLS 握手协议的丛，R_s 为服务器对客户端的测试元素，节点$\{S_1, S_2\} \subset \mathcal{E}$，且 $S_1 \Rightarrow^{+} S_2$ 为 R_s 的一个 DH 参数签名测试，则必然存在正规的客户端节点$\{C_1, C_2\} \subset \mathcal{E}$使得满足$[|*, R_s, *, d_2, *|]_{Kc} \in t$ 的 t 是 C_2 的一个元素，且对于 R_s 来说，$C_1 \Rightarrow^{+} C_2$ 是一条转换边。

命题 1 和命题 2 的正确性同定理 1。它们描述了客户端和服务器都参与了同一轮协议运行，相互认证并提供临时的认证和密钥协商参数。

结论 1　TLS 握手协议满足认证属性。

4.3　TLS 握手协议保密性分析

首先，分析实体的长期签名密钥的保密性。

命题 3　令$\mathcal{E}$是包含 TLS 握手协议的丛，由图 3 可见，不存在节点 $n \in \mathcal{E}$使得 $K \in K_{Sig}$ 的 $K \notin term(n)$，且 $K \notin K_{P0}$，那么 $K \notin K_P$。

证明　命题 3 的正确性取决于 Dolev-Yao 假设[17]，即假设入侵者不能通过签名消息恢复出签名密钥。命题 3 描述的是正规实体的长期签名密钥不作为消息项在信道上发送，且不属于入侵者初始密钥集，那么实体的长期签名密钥必然不属于可入侵密钥集。

然后，提出会话主密钥的保密属性。

命题 4　令$\mathcal{E}$是包含 TLS 握手协议的丛，且 TLS 握手协议满足保守性(conservative)和沉默性(silent)[15]，存在正规节点 S_1 和 C_2 有 $d_1 \in term(S_1)$，$d_2 \in term(C_2)$，且不存在正规节点 n 使得 $DH \in term(n)$，这里 $DH=d_1 \times d_2$。那么会话主密钥 $SK \notin K_P$。

证明　命题 4 的证明见文献[15]。

结论 2　TLS 握手协议满足保密性。

5　结束语

在 Jonathan C.Herzog 的研究工作基础上，结合串空间基本理论和认证测试的思想对 TLS 协议 1.2 版本进行分析，建立了该协议的认证测试模型，分析和证明了它的保密性和认证性等关键属性。结果表明 TLS 协议满足其安全性说明。

TLS 协议是一种复杂的传输层安全协议，包含两层协议，并提供三种认证和密钥协商方法，限于篇幅，分析了其中一种较为通用的认证和密钥协商方法，完整的协议分析有待进一步的工作。

参考文献：

[1] RFC 2246.The TLS protocol version 1.0[S].1999.

[2] RFC 5246.The TLS protocol version 1.2[S].2008.

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

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

[5] Thayer F J，Herzog J C，Guttman J D.Strand spaces：Proving security protocols correct[J].Journal of Computer Security，1999，7(2/3)：191-230.

[6] 蒋睿，胡爱群，李建华. 基于 Authentication Test 方法的高效安全 IKE 形式化设计研究[J].计算机学报，2006，29(9)：1694-1701.

[7] 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(1)：148-156.

[8] 卢凤清，林东岱.认证测试的一个扩展[J].中国科学院研究生院学报，2007，24(4)：488-493.

[9] 方燕萍，章晓芳，张广泉.串空间模型及其认证测试方法的一种扩展与应用[J].计算机应用，2008，28(12).

[10] Paulson L C.Inductive analysis of the Internet protocol TLS[J].ACM Transactions on Computer and System Security，Computer Laboratory University of Cambridge，1999：332-351.

[11] Calixto A，Monroy R.TLS analysis using cadp[J].Studia Informatica Universalis，2001.

[12] Ogata K，Futatsugi K.Equational approach to formal analysis of TLS [C]//Proceedings 25th IEEE International Conference on Distributed Computing Systems(ICDCS 2005).Columbus，OH，USA：IEEE Computer Society Press，2005：795-804.

[13] 孙红林，叶顶锋，吕述望，等.传输层安全协议的安全性分析及改进[J].软件学报，2003，14(3)：518-523.

[14] 倪阳，张玉清.TLS 握手协议的计算模型分析[J].中国科学院研究生院学报，2008，25(1)：110-116.

[15] Herzog J C.The diffie-hellman key-agreement scheme in the strand-space model[C]//Proceedings of the 16th IEEE Computer Security Foundations Workshop(CSFW'03)，IEEE Computer Society，2003：234-247.

[16] RFC 5280.Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL)Profile[S].2008.

[17] Dolev D，Yao A C.On the security of public key protocols[J].IEEE Transactions on Information Theory，1983，29(2)：198-208.

(上接 54 页)

[4] Chalkiadakis G，Boutilier C.Coordination in multiagent reinforcement learning：A bayesian approach[C]//AAMAS'03，Melbourne，Australia，2003，7：14-18.

[5] Cao Y U，Fukunaga A S，Kahng A B.Cooperative mobile robotics：Antecedents and directions[J].Autonomous Robots，1997，4：1-23.

[6] Wang X，Sandholm T.Reinforcement learning to play an optimal nash equilibrium in team markov games[C]//Neural Information Processing Systems，2002：1571-1578.

[7] 宋梅萍，顾国昌，张国印，等.一般和博弈中的合作多 Agent 学习[J].控制理论与应用，2007，24(2)：317-321.

[8] Fulda N，Ventura D.Predicting and preventing coordination problems in cooperative learning systems[C]//Proceedings of the International Joint Conference on Artificial Intelligence，Hyderabad，India，2007.