第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·博士论文· 文章编号：1000—3428(2007)20—0030—04 文献标识码：A 中图分类号：TP309

# 一种可分析保密性与认证性的模态逻辑

赵华伟[1]，秦 静[2]
(1. 山东财政学院计算机信息工程学院，济南 250014；2. 山东大学数学与系统科学学院，济南 250100)

**摘 要：**提出了一种新的基于信念的模态逻辑——MBL 逻辑，来分析由单向函数构造的对称钥认证交换协议的安全性。该逻辑有严格的证明体系，可证明推理规则在其语义模型下的正确性，说明该逻辑具有合理性。其推理规则不仅能对单向函数保护的消息进行有关认证性的推理，克服了以往逻辑系统使用不当的安全服务来分析协议认证性的缺陷，而且可分析消息的保密性，避免了其他逻辑分析协议时对可信中心的过分依赖，可发现敌手通过欺骗可信中心而造成的攻击。

**关键词：**模态逻辑；MBL 逻辑；BAN 类逻辑；会话密钥

# Modal Logic for Analyzing Privacy and Authentication

ZHAO Hua-wei[1], Qin Jing[2]
(1. School of Computer Information Engineering, Shandong University of Finance, Jinan 250014;
2. School of Mathematics and System Science, Shandong University, Jinan 250100)

**【Abstract】** A modal logic based on belief, MBL logic, is introduced to analyze security of authentication key-exchange protocols with one-way functions. The logic has following characteristics: it has a rational proof system and its inference rules can be proved right under its own semantic model. It can analyze authentication of messages protected by one-way functions, and analyze whether messages are kept secret. Through these rules, analyzer could reduce the dependency on trusted third part about the security of temporary session key, and be able to find whether adversaries could make effective attacks on protocols through cheating trusted third part.

**【Key words】** modal logic; MBL logic; BAN-like logic; session key

作为一类著名的安全协议形式化分析方法，BAN类逻辑曾分析并验证了许多重要的安全协议，例如Needham-Schroeder对称钥协议、Nessett协议等。但这类逻辑仍存在若干缺陷，例如采用错误的安全服务来分析认证性，缺少保密性的描述，没有关于系统合理性的严格证明机制等。本文介绍的MBL逻辑对这些缺陷一一作了改进：(1)它拥有关于单向函数的推理规则，能够采用正确的安全服务来分析消息的认证性；(2)拥有保密性的推理规则，从而避免主体由于过分信赖可信中心而受到敌手的攻击；(3)其推理规则在其语义模型下可证明是正确的，说明了该逻辑系统的合理性[1~4]。

## 1 BAN 类逻辑的缺陷

**缺陷 1** 理想化方法不规范

BAN 逻辑在分析安全协议时要进行理想化处理，以便将协议的一般说明转化为可被逻辑系统所理解的形式，并表达消息的内在含义。但这种理想化方法缺少规范化手段，需要分析者对协议充分理解并依靠经验来完成，这样就会产生安全隐患。例如下面的协议：

$(1)A\rightarrow B:A,Na$
$(2)B\rightarrow S:A,Na,B,Nb$
$(3)S\rightarrow B:\{Kab,Nb\}_{Kbs},\{Kab,Na\}_{Kas}$
$(4)B\rightarrow A:\{Kab,Na\}_{Kas},\{Na\}_{Kab},Nb'$
$(5)A\rightarrow B:\{Nb'\}_{Kab}$

按照 BAN 逻辑的理想化过程，协议第 3 步的理想化应为 $S\rightarrow B:\{A\xleftrightarrow{Kab}B,\#(A\xleftrightarrow{Kab}B),Nb\}_{Kbs},\{A\xleftrightarrow{Kab}B,Na\}_{Kas}$，当 $B$ 收到 $\{Kab,Nb\}_{Kbs}$ 后，通过理想化步骤中的 $\{A\xleftrightarrow{Kab}B,\#(A\xleftrightarrow{Kab}B),Nb\}_{Kbs}$ 便认为 $Kab$ 是 $A$、$B$ 间的良好临时会话密钥。采用 BAN 逻辑对理想化后的协议进行分析，就会得出该协议是安全的结论。

但是该协议并不安全，敌手通过欺骗可信中心 $S$ 就能发起冒充攻击，攻击步骤如下：

$(1)E(A)\rightarrow B:A,Na$
$(2)B\rightarrow S:E(A),Na,B,Nb$
$(3)S\rightarrow B:\{Kab,Nb\}_{Kbs},\{Kab,Na\}_{Kes}$
$(4)B\rightarrow E(A):\{Kab,Na\}_{Kes},\{Na\}_{Kab},Nb'$
$(5)E(A)\rightarrow B:\{Nb'\}_{Kab}$

第 1 步，攻击者 $E$ 冒充 $A$ 给 $B$ 发出通信请求；第 2 步 $E$ 将 $B$ 发出消息中的主体标示符“$A$”改为“$E$”来欺骗 $S$。第 4 步，$E$ 截获 $B$ 发给 $A$ 的消息 $\{Kab,Na\}_{Kes}$，解出其中的会话密钥 $Kab$；第 5 步，$E$ 将 $\{Nb'\}_{Kab}$ 发给 $B$，使得 $B$ 误认为 $A$ 拥有 $Kab$。这样 $E$ 就能冒充 $A$ 来和 $B$ 进行通信了。

**缺陷 2** 安全服务的误用

BAN 类逻辑在分析认证性时采用了错误的安全服务，即利用保密服务来推理认证性。由于没有受到完整性保护的密文会被敌手篡改，保密服务并不能提供消息源的确认。例如，文献[5]描述的一种对 Needham-Schroeder 对称钥认证协议的攻击。在该攻击中，敌手对采用 AES-CBC 算法的密文进行有意义的修改，而接收方认为修改后的消息仍是来自发方的完好消息。该攻击说明，若密文没有受到完整性保护，解密者就不能确信解密数据的真实性。由此看出，保密服务无法提供有效的消息源认证。

**基金项目：**国家“863”计划基金资助项目(2003AA141120，2004AA001260)；山东省自然科学基金资助项目(Y2003A03)
**作者简介：**赵华伟(1977－)，男，博士、讲师，主研方向：信息安全；秦 静，博士、教授
**收稿日期：**2006-12-05 **E-mail：**zhuav@163.com

**缺陷 3** 缺少证明系统合理性的严格机制

BAN 类逻辑中的 BAN 逻辑与 GNY 逻辑都没有提供独立且明确的语义基础，造成逻辑系统缺乏合理性的依据，因此受到很多质疑。鉴于此，AT 逻辑与 SVO 逻辑均给出了语义模型，为逻辑系统的合理性打下了基础。但在 AT 逻辑与 SVO 逻辑中，推理逻辑都以公理的形式给出，而公理无需证明，因此对于逻辑公理与语义模型间的正确联系仍无法判断。

## 2 MBL 逻辑

在弥补 BAN 类逻辑的不足的基础上，本文为具有认证性的对称钥交换协议建立了一种系统的、切合实际的形式化分析工具：MBL 逻辑。

### 2.1 MBL 逻辑的符号

$A$、$B$、$P$ 为主体，$S$ 为可信中心，$E$ 为敌手，$M$ 为消息集合，$m$ 为消息元素；$\odot M$ 表示 $M$ 具有完整性；$M_B$ 表示 $B$ 曾发出过 $M$；$(\odot M)_B$ 表示 $B$ 曾发出过 $M$，且 $M$ 具有完整性；$\phi,\varphi$ 代表公式；$A\ bels(\phi)$ 表示 $A$ 相信 $\phi$；$\otimes_{A\leftrightarrow B}M$ 表示 $M$ 在 $A$、$B$ 间保密；$good1(K,A,B)$ 表示 $K$ 为 $A$、$B$ 间的保密密钥；$good2(K,A,B)$ 表示 $K$ 为 $A$、$B$ 间新鲜的保密密钥；$good(K,A,B)$ 表示 $good1(K,A,B)$ 或 $good2(K,A,B)$；$_{A\leftrightarrow B}K$ 表示 $K$ 是为 $A$ 和 $B$ 产生的密钥；$\{M\}_K$ 表示用 $K$ 对 $M$ 的加密；$[M]_K$ 表示用带密钥 $K$ 的单向函数对 $M$ 进行的单向变换，其中 $[M]_K=(M,prf_K(M))$，$prf_K(\ )$ 在对称钥加密的实现中表示带密钥的伪随机函数；$A\ verifies[M]_K$ 表示 $A$ 用 $K$ 对 $[M]_K=(M,prf_K(M))$ 验证通过；其他符号在语义模型中给出。

### 2.2 MBL 逻辑的语义模型

每个主体 $P$ 有一个本地状态 $S_P$，它是一个多维向量族 $(B_P,Send_P,Receive_P,H_P)$，其中，$B_P$ 是主体 $P$ 的信念集合；$Send_P$ 是 $P$ 曾经说过消息的集合，包括自己产生的消息和转发的消息；$Receive_P$ 是 $P$ 曾经收到消息的集合；$H_P$ 是 $P$ 所拥有消息的集合。本文认为任何主体都可区分自己产生的消息和他人产生的消息。

全局状态包括所有主体局部状态的向量族 $(st_1,st_2,\cdots,st_n)$，还包括一个全局的公开消息集合 $public()$：所有公开的消息与消息集的集合。MBL 逻辑中还隐含着一个秘密消息集合，集合中消息的保密性是通过公开集合 $public()$来描述的。所有的集合都是单调、递增和闭包的。

定义一轮协议 $r$ 是一个由整数时间索引的全局变量的有限集合，协议中的 $t$ 记为 $(r,t)$。定义 $V$ 为原始命题集合，定义 $\pi$ 为一映射，将每一个常量命题 $v\in V$ 映射为点集 $\pi(v)$，即命题 $v$ 为真的点。公式 $\Psi$ 在点 $(r,t)$ 为真记为：$(r,t)\models\Psi$，$\models\Psi$ 代表 $\Psi$ 全真。

为了描述公式的语义，首先给出基本的逻辑关系和一些基本公理。

(1)基本逻辑关系

$(r,t)\models v\ \ iff\ \ if\ \ v\in V,then\ \ (r,t)\in\pi(v)$

$(r,t)\models(\phi\varphi)\ \ iff\ \ (r,t)\models\phi\wedge\varphi$

$(r,t)\models\phi\wedge\varphi\ \ iff\ \ (r,t)\models\phi\wedge(r,t)\models\varphi$

$(r,t)\models(\phi\rightarrow\varphi)\ \ iff\ \ (r,t)\models\phi\rightarrow(r,t)\models\varphi$

(2)基本公理

**公理 1** 主体的发送集合与接收集合都属于主体的拥有集合。

$\models Send_P\subset H_P$；$\models Receive_P\subset H_P$

**公理 2** 若主体拥有 $\phi$，则主体相信自己拥有 $\phi$。

$\phi\in H_P\supset(\phi\in H_P)\in B_P$

**公理 3** 若 $M$ 和 $M'$ 均为消息，则 $M\rightarrow M'$ 和 $f(M)\rightarrow M'$ 意味着 $M'$ 为 $M$ 的元素或子集合（$f$ 为 $M$ 的一个映射）。

$M\rightarrow M'\ or\ f(M)\rightarrow M'\ \ iff\ \ M'\subset M$

**公理 4** 信任关系

$\phi\in B_P\wedge\varphi\in B_P\supset\phi\wedge\varphi\in B_P$

**公理 5** 当主体发送或接收一个复合消息，则发送或接收其子消息

$(m_1,m_2)\in Send_P\supset m_1\in Send_P\wedge m_2\in Send_P$

$(m_1,m_2)\in Receive_P\supset m_1\in Receive_P\wedge m_2\in Receive_P$

**公理 6** 完整性

$\odot(m_1,m_2)\supset\odot m_1\wedge\odot m_2$

(3)逻辑公式的语义

**语义 1** 看到

$(r,t)\models A\ sees(M)\ \ iff\ \ (r,t)\models M\in H_A\ \ or\ (r,t)\models K\in H_A\wedge\{M\}_K\in H_A$

**语义 2** 诉说

$(r,t)\models A\ says(x)\ \ iff\ \ (\exists 0<t'\le t)\ (r,t')\models x\in Send_A$

$(r,t)\models A\ said(x)\ \ iff\ \ (\exists t'\le t)\ (r,t')\models x\in Send_A$

$(r,t)\models M_B\ \ iff\ \ (r,t)\models B\ said(M)$

**语义 3** 新鲜性

$(r,t)\models fresh(x)\ \ iff\ \ \forall P,\ \forall t'<0,\ (r,t')\neq P\ said(x)$

**语义 4** 公开性

$(r,t)\models M\in public()\ \ iff\ \ \forall t,\forall P,(r,t)\models P\ \ sees(M)$

**语义 5** 完整性

$(r,t)\models\odot M\ \ iff\ \ \exists P,(r,t)\models P\ \ verifies[M]_K$

**语义 6** 被传递消息的保密性

1)对于一个消息集合 $M$

$(r,t)\models\otimes_{A\leftrightarrow B}M\ \ iff\ \ \exists K,(r,t)\models good(K,A,B)\wedge\odot\{M\}_K$

2)对于一个原子消息 $m$

$(r,t)\models\otimes_{A\leftrightarrow B}m\ \ iff\ \ \exists M,\ (r,t)\models\otimes_{A\leftrightarrow B}M\wedge m\in M\wedge m\notin public()$

**语义 7** 属于

$(r,t)\models m\in M\ \ iff\ \ \exists P,\ (r,t)\models m\in H_P\wedge(M=m_1\cdots m\cdots)\in H_P\ \ or\ \ K\in H_P\wedge(M=\{m_1\cdots m\cdots\}_K)\in H_P$

**语义 8** 保密会话密钥

$(r,t)\models good1(K,A,B)\ \ iff\ \ (r,t)\models\otimes_{A\leftrightarrow B}K$

$(r,t)\models good2(K,A,B)\ \ iff\ \ (r,t)\models fresh(K)\wedge\otimes_{A\leftrightarrow B}K$

**语义 9** 可信中心管辖密钥

$(r,t)\models S\ \ controls(K)\ \ iff\ \ \exists P$

$if\ (r,t)\models P\ \ bels(S\ \ says(M,A,B))\wedge P\ \ bels(K\in M)$

$then\ \ (r,t)\models P\ \ bels(fresh(K))\wedge P\ \ bels(_{A\leftrightarrow B}K)$

**语义 10** 验证单向函数

$(r,t)\models A\ \ verifies[M]_K\ \ iff\ \ (r,t)\models(M\in public()\wedge\odot M)\in B_A\wedge$

$if\ \ (r,t)\models(good(K,A,B))\in B_A\wedge[M]_K\in Receive_A$

$then\ \ (B\ \ said[M]_K\wedge K\in H_B)\in B_A$

**语义 11** 具有消息来源的完整性

$(r,t)\models(\odot M)_A\ \ iff\ \ \exists t'\le t,(r,t')\models M\in Send_A\wedge\odot M$

### 2.3 推理规则

(1)可识别消息来源的完整性规则

$A\ bels(good(K,A,B))\wedge A\ verifies[M]_K\supset$

$A\ bels(\odot M)_B\wedge A\ bels(M\in public())\wedge A\ bels(K\in H_B)$

当 $A$ 相信 $K$ 为 $A$、$B$ 间的良好会话密钥。且 $A$ 验证单向函数成功后，$A$ 相信 $M$ 是来自 $B$ 的具有完整性的公开消息，且相信 $B$ 拥有 $K$。

推论：$A\ bels(\odot M)_B \supset A\ bels(\odot M) \wedge A\ bels(M_B)$

(2)消息提取规则

1)$A\ bels(M) \wedge A\ bels(m \in M) \supset A\ bels(m)$

2)$A\ bels(\odot M)_B \wedge A\ bels(m \in M) \supset A\ bels(\odot m)_B$

3)$A\ says(M) \wedge A\ bels(m \in M) \supset A\ says(m)$

(3)消息合取规则

$A\ bels(\odot m_i)_B \wedge A\ bels(\odot m_j)_B \supset A\ bels(\odot(m_i m_j))_B$

(4)新鲜性规则

$A\ bels(\ fresh(m) \wedge A\ bels(m \in M)) \supset A\ bels(\ fresh(M))$

(5)新鲜性验证规则

$A\ bels(\odot M)_B \wedge A\ bels(\ fresh(M)) \supset A\ bels(B\ says(M))$

(6)良好临时会话密钥判定规则($S$ 为可信中心)

$A\ bels(good1(K,A,S)) \wedge A\ bels(S\ \ says(M,A,B)) \wedge$
$A\ bels(K \in M) \wedge A\ bels(S\ \ controls(K)) \supset A\ bels(good2(K,A,B))$

当 $A$ 相信 $K$ 在 $S$、$A$ 间秘密共享，且相信 $S$ 刚刚发布了包含有 $K$ 和会话双方标示符的消息，则 $A$ 相信 $K$ 的确是为 $A$ 和 $B$ 颁发的新鲜的临时会话密钥(此时 $B$ 也许还没有得到 $K$)。

(7)保密性规则

$A\ bels(good(K,A,B)) \wedge A\ bels \odot \{M\}_K \wedge$
$A\ bels(m \notin public()) \wedge A\ bels(m \in \{M\}_K) \supset A\ bels(\otimes_{A \leftrightarrow B} m)$

$A$ 同时相信 $K$ 为 $A$、$B$ 间的秘密会话密钥，加密消息 $\{M\}_K$ 具有完整性，和 $m$ 是 $M$ 中未公开的消息，那么 $A$ 相信 $m$ 是在 $A$、$B$ 间秘密共享的。

(8)拥有即相信规则

$M \in H_A \supset A\ bels(M \in H_A)$

### 2.4 正确性证明

对 BAN 类逻辑一个争议焦点是它们缺乏有效的正确性证明机制。在 MBL 逻辑中，所有推理规则在其语义模型与公理下都是正确的，本文仅举例证明规则 2 的正确性。

可识别消息来源的完整性规则的正确性证明：

$A\ bels(good(K,A,B)) \wedge A\ \ verifies[M]_K \supset$
$A\ bels(\odot M)_B \wedge A\ bels(M \in public()) \wedge A\ bels(K \in H_B)$

证明

左边 $\equiv (r,t) \models (good(K,A,B)) \in B_A \wedge (r,t) \models (M \in public() \wedge \odot M) \in B_A \wedge$
$\quad if\ \ (r,t) \models (good(K,A,B)) \in B_A \wedge [M]_K \in Receive_A$
$\quad then\ \ (r,t) \models (B\ \ said[M]_K \wedge K \in H_B) \in B_A$

语义10
$\Rightarrow (r,t) \models (M \in public() \wedge \odot M) \in B_A \wedge ([M]_K \in Send_B)$
$\in B_A \wedge (K \in H_B) \in B_A$

公理3
$\Rightarrow (r,t) \models (M \in public() \wedge \odot M) \in B_A \wedge (M \in Send_B)$
$\in B_A \wedge (K \in H_B) \in B_A$

公理4
$\Rightarrow A\ bels(\odot M)_B \wedge A\ bels(M \in public()) \wedge A\ bels(K \in H_B) \equiv$ 右边

注：由于 $A$ 能够识别自己的消息和外来消息，因此 $A$ 可以判断 $[M]_K$ 是接收的消息。

## 3 分析举例

本文将分析一种改进后的 Needham-Schroeder 对称钥认证交换协议，其中只对含有密码运算结果的消息进行分析，不需进行理想化处理。

(1)$A \rightarrow B: N_A, A$

(2)$B \rightarrow S: N_A, N_B, A, B$

(3)$S \rightarrow B: [\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}, [\{K\}_{K_{AS}}, N_A, A, B]_{K_{AS}}$

(4)$B \rightarrow A: [\{K\}_{K_{AS}}, N_A, A, B]_{K_{AS}}$

(5)$A \rightarrow B: [N_A']_K$

(6)$B \rightarrow A: [N_A'-1]_K$

前提假设

$A\ bels(good1(K_{AS}, A, S))$；$A\ bels(\ fresh(N_A))$；
$A\ bels(S\ controls(K))$；$B\ bels(good1(K_{BS}, B, S))$；
$B\ bels(\ fresh(N_B))$；$B\ bels(S\ controls(K))$；
$A\ bels(\{A, B, N_A, N_A'\} \subset public())$；
$A\ bels(\{A, B, N_A, N_A', K_{AS}\} \subset H_A)$
$B\ bels(\{A, B, N_B\} \subset public())$；$B\ bels(\{A, B, N_B, K_{AS}\} \subset H_B)$
$S\ bels(good1(K_{AS}, A, S))$；$S\ bels(good1(K_{BS}, B, S))$

目标：

$A\ bels(good2(K, A, B))$；$A\ bels(K \in H_B)$；
$B\ bels(good2(K, A, B))$；$B\ bels(K \in H_A)$

形式化分析：

协议第 3 步，当 $B$ 收到消息 $[\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}$ 后，用 $K_{BS}$ 对消息 $[\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}$ 验证通过后，运用可识别消息来源的完整性规则：

$B\ bels(good(K_{BS}, B, S)) \wedge B\ \ verifies([\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}) \supset$
$B\ bels(\odot(\{K\}_{K_{BS}}, N_B, A, B))_S \wedge B\ \ bels((\{K\}_{K_{BS}}, N_B, A, B) \in public())$ (1)

由公理 1 和基本逻辑关系得

$([\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}) \in Receive_B \supset ([\{K\}_{K_{BS}}, N_B, A, B]_{K_{BS}}) \in H_B$
$\supset \{K\}_{K_{BS}} \in H_B$ (2)

对式(2)运用拥有即相信规则可得

$B\ \ bels((\{K\}_{K_{BS}}, N_B, A, B) \in H_B)$，$B\ \ bels(\{K\}_{K_{BS}} \in H_B)$ (3)

对式(3)运用公理 4 和属于语义，可得

$B\ \ bels((\{K\}_{K_{BS}}, N_B, A, B) \in H_B) \wedge B\ \ bels(\{K\}_{K_{BS}} \in H_B)$
$\supset B\ \ bels(\{K\}_{K_{BS}} \in (\{K\}_{K_{BS}}, N_B, A, B)$ (4)

对式(1)和式(4)运用消息提取规则可得

$B\ bels(\odot\{K\}_{K_{BS}})_S \supset B\ bels(\odot\{K\}_{K_{BS}})$ (5)

结合前提假设 $K_{BS} \in H_B$ 和式(2)，由属于语义可得：

$K_{BS} \in H_B \wedge \{K\}_{K_{BS}} \in H_B \supset K \in \{K\}_{K_{BS}}$ (6)

由式(6)，根据拥有即相信规则和语义 7 可得

$B\ \ bels(K \in H_B) \wedge B\ \ bels(\{K\}_{K_{BS}} \in H_B)$
$\supset B\ \ bels(K_{BS} \in H_B \wedge \{K\}_{K_{BS}} \in H_B)$
$\supset B\ \ bels(K \in \{K\}_{K_{BS}})$ (7)

此时，$B$ 并没有将 $K$ 加入 $public()$集合，所以有

$B\ \ bels(K \notin public())$ (8)

由前提假设 $B\ \ bels(good2(K_{BS}, B, S))$、式(5)、式(7)、式(8)，根据保密性规则可得

$B\ \ bels(good2(K_{BS}, B, S)) \wedge B\ bels(\odot\{K\}_{K_{BS}})$
$\wedge B\ bels(K \in \{K\}_{K_{BS}}) \wedge B\ \ bels(K \notin public()) \supset B\ \ bels(\otimes_{B \leftrightarrow S} K)$ (9)

由前提假设 $N_B \in H_B$ 和式(2)，根据拥有即相信规则和语义 7 可得

$B\ \ bels(N_B \in H_B) \wedge B\ \ bels((\{K\}_{K_{BS}}, N_B, A, B) \in H_B) \supset$
$B\ \ bels(N_B \in (\{K\}_{K_{BS}}, N_B, A, B))$ (10)

由前提假设 $B\ \ bels(\ fresh(N_B))$ 和式(10)，根据新鲜性规则可得

$B\ \ bels(\ fresh(\{K\}_{K_{BS}}, N_B, A, B))$ (11)

由式(1)和式(11)，根据新鲜性验证规则可得

$B\ \ bels(\odot(\{K\}_{K_{BS}}, N_B, A, B))_S \wedge B\ \ bels(\ fresh(\{K\}_{K_{BS}}, N_B, A, B)) \supset$
$B\ \ bels(S\ \ says(\{K\}_{K_{BS}}, N_B, A, B))$ (12)

由前提条件：$B\ \ bels(S\ \ controls(K))$ 和式(7)、式(9)、式(12)，根据良好临时会话密钥判定规则可得

$$B\ bels(S\ controls(K)) \wedge B\ bels(K \in \{K\}_{K_{BS}}) \wedge B\ bels(\otimes_{B \leftrightarrow S} K) \wedge B\ bels(S\ says(\{K\}_{K_{BS}}, N_B, A, B)) \supset B\ bels(good2(K, A, B)) \quad (13)$$

在协议的第 5 步，当 $B$ 结合式(13)验证 $[N_A']_K$ 通过后，运用可识别消息来源的完整性规则：

$$B\ bels(good2(K, A, B)) \wedge B\ verifies([N_A']_K) \supset B\ bels(K \in H_A) \quad (14)$$

通过以上推理可得出结论：

$B\ bels(good2(K, A, B))$， $B\ bels(K \in H_A)$

同理可得结论：

$A\ bels(good2(K, A, B))$， $A\ bels(K \in H_B)$

在协议结束时主体的信念符合协议的预定目标，因此协议是安全的。

## 4 结论

本文在 BAN 类逻辑的基础上，构造了一个具有详细计算模型和语义模型的形式化分析工具——MBL 逻辑，来分析基于单向函数的对称钥认证交换协议。与 BAN 类逻辑相比它有以下特点：

(1)增加了保密性的语义说明和推理规则，主体可自主分析消息的保密性，因此能减少对可信中心的依赖，防止敌手通过欺骗可信中心而造成的攻击。

(2)增加了单向函数的推理规则，使得 MBL 逻辑采用了正确的安全服务来分析消息的认证性。

(3)具有详细的语义模型，并且推理规则在该语义模型下可证明是正确的。

### 参考文献


1 Burrows M, Abadi M, Needham R. A Logic of Authentication[R]. Digital Systems Research Center, Research Report 39, 1989.

2 Gong L, Needham R, Yahalom R. Reasoning about Belief in Cryptographic Protocols[C]//Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press.1990.

3 Abadi M, Tuttle M R. A Semantics for a Logic of Authentication[C]//Proceedings of the 10th ACM Symposium on Principles of Distributed Computering. 1991.

4 Syverson P F, Van Oorschot P C. On Unifying Some Cryptographic Protocol Logics[C]//Proceedings of the 1994 IEEE Computer Society Symposium on Research Insecurity and Privacy. Los Alamitos: I EEE Computer Society Press. 1994.

5 毛文波. 现代密码学理论与实践[M]. 北京：电子工业出版社, 2004.


(上接第 26 页)

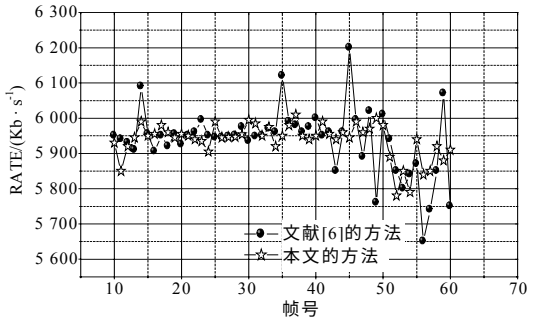


**图 8　本文方法同文献[6]方法码率输出曲线比较**

## 4 结束语

本文主要考虑的是有线网络环境，而对于无线网络，影响其的主要因素是丢包率，在本文的基础上研究无线网络的应用也将是有意义的探索。

### 参考文献


1 ISO/IEC International Standard 13818-2-1995. Generic Coding of Moving Pictures and Associated Audio Information:Video[S]. 1995.

2 ISO/IEC International Standard 14496-2-1999. Information Technology Generic Coding of Audio-visual Objects[S]. 1999.

3 Wu F, Li S, Zhang Y Q. A Framework for Efficient Progressive Fine Granularity Scalable Video Coding[J]. IEEE Trans. on Circuit and Systems for Video Technology, Special Issue on Streaming Video, 2001, 11(3): 332-344.

4 Ding G G, Guo B L. Improvement to Progressive Fine Granularity Scalable Video Coding[J]. Computational Intelligence and Multimedia Applications, 2003, 27(30): 249-253.

5 Stewart R, Xie Q, Morneault K, et al. Stream Control Transmission Protocol[Z]. (2000-10). http://www.ietf.org/rfc/rfc2960.txt.

6 张　方, 吴成柯, 程培星, 等. 一种改进的可分级视频编码方法及其网络传输研究[J]. 电子与信息学报, 2005, 27(1): 108-111.

7 Zhang Q, Zhu W W, Zhang Y Q. Resource Allocation for Multimedia Streaming over the Internet[J]. IEEE Trans. on Multimedia, 2001, 3(3): 339-355.


(上接第 29 页)

面：(1)从符号表达式方面入手，继续寻找内存占用率较小的表示方法，例如 MDG、*BMD 等。(2)扩充轨迹逻辑的表达能力，STE 只能描述向后的特性，虽然 GSTE 对其进行了扩充，但也不能描述与并发行为有关的特征，因而使 STE 具有并发刻画能力是下一个研究方向。(3)基于符号模拟的系统诊断和纠错。传统的纠错方式首先通过其他验证技术得到错误向量，然后由错误向量推断错误出现的可能位置，采用符号模拟的方法可以将两者合为一个过程，在测试的同时就可进行诊断和纠错。

### 参考文献


1 Carter W C, Joyner Jr W H, Brand D. Symbolic Simulation for Correct Machine Design[C]//Proc. of ACM/IEEE Design Automation Conference. 1979: 280-286.

2 Bryant R E. Symbolic Verification of MOS Circuits[C]//Proc. of Chapel Hill Conference on VSLI. 1985: 419-438.

3 Bryant R E. A Method for Hardware Verification Based on Logic Simulation[J]. Journal of the ACM, 1991, 38(2): 299-328.

4 Wilson C, Dill D L, Bryant R E. Symbolic Simulation with Approximate Values[C]//Proc. of the 3rd International Conference on Formal Methods in Computer-aided Design. 2000: 470-485.

5 Zeng Z, Talupuru K R, Ciesielski M. Functional Test Generation Based on Word-level SAT[J]. Journal of Systems Architecture, 2005, 51(8): 488-511.

6 Aagaard M D, Jones R B, Seger C H. Formal Verification Using Parametric Representations of Boolean Constraints[C]//Proc. of Design Automation Conference. 1999: 402-407.