关于 BAN 逻辑的语义模型的分析与改进[1]

费定舟　邓达强

（中山大学逻辑与认知研究所，广州 510275）

摘要：本文针对 BAN 逻辑及其语义模型的不足之处，提供了我们的改进后的定义，它比 BAN 原作者们所提供的信念定义显得更合理些。

关键词：Authentication logic;　BAN 逻辑；语义模型

中图分类号：B81　　文献标识码：A

1、引言

Internet 以及 e－Commerce 的发展要求不断提高通信过程和信息的安全性。密码学的重要任务之一是研究设计并开发高安全性的认证方法和系统。其中，安全协议是一个关键领域．从逻辑形式结构方面研究安全协议，开拓性工作是 BAN 逻辑系统［Burrows, M., Abadi, M., Needham, R., 1990］，以较为严密和应用的普遍性见长，因为并不需要过多的细节。它可以对两个重要的工业安全协议应用 GSM(Global System for Mobil Communication) [Gunnar , H., 1999]和 SET (Secure Electronic Transactions)提供直觉和足够的解释力［Agray, N., vonder Hoek, E., de vink, 2002］。目前，BAN 逻辑成为研究密码和安全协议的广泛采用的形式化工具。就 BAN 逻辑本身而言，近十年来重点放在它的模态变种及其理论模型方面。其语义模型正处于不断的改进和修改之中，这方面的工作见[Abadi, M., Tuttle, M., 1991; Gong, L., Needham, R., Yahalom, R., 1991; Wedel, G., Kessler, V., 1996]。

本文讨论 BAN 逻辑的语义模型。与以 GNY[Gong, L., Neddham, R., Yahalom, R., 1990] 为代表的工作不同，他们讨论 Beliefs 与 Know 之间的逻辑联系，我们考察 Belief 的模型定义并分析其不足之处，相应地给出我们关于 Belief 的新定义，它能提供直觉上和推理上的更合理的说明。

2、BAN 逻辑

2.1 Authentication 是确定参加通信的实体的身份的计算行为，在安全协议中起非常重要的作用。一个认证协议（Authentication protocol）告诉我们 secret 如何分配给这些实体，以及如何确定其身份的。认证逻辑则抽掉认证过程的诸多细节如算法和数学的细节，保留反映安全问题的逻辑上的特征和结构［白硕等，2000］，考察中参与认证协议中各实体信念问题，建立起相应的形式化系统。BAN 逻辑则是这些形式化系统中研究较多的一种。下面介绍改进后的 BAN 逻辑形式系统。

2.2 先从直观上引进几个认证协议中常用的几个概念。

实体：P，Q，R，S

加密密钥：K

公式：X，Y

消息： m，M，X，Y

P believes X：P 相信 X 是真的，而 X 本身既真既假，但 P 把 X 当做真的。

P see X：P 已经接收到消息 X。假如 P 有相应的解密密钥，那么他能够读出它的内容，同时 P 亦把 X 发送给其它实体。

P said X：P 已经发送消息 X，P 相信他发送的 X 是真的。

P controls X：P 对 X 有判定权，即 P 是对 X 的真的可信任的当局。

fresh(X)：X 是新鲜的。时间分为两个时段：过去与现在。而现在则以当前协议执行的起点为起点。当 X 不包含在过去发送的消息中，X 是新鲜的。

$P \leftrightarrow^{K} Q$：K 是 P 和 Q 的公钥。K 是 P、Q 之间通信的安全密钥，除 P、Q 之外，其它实体包括 P、Q 信任的实体都不能破译。

$P \ \#^{x} Q$：X 是 P 和 Q 的公钥密钥。X 是只有 P、Q 知道的密文（如 passwod），其它实体如 P、Q 所信任的实体可能知道 X。P 和 Q 用 X 来证明它们的身份。

$\{X\}_K$：X 以 K 加密，$\{X\}_K$ 表示以 K 加密于 X 后的消息。它是的 $\{X^P\}_K$ 简写，P 表示消息发送源的实体。有时省略 P 是为了表明每个实体能够识别属于自己的消息。

$<X>_Y$：X 与 Y 的结合。$<X>_Y$ 表示这样的消息 X，它与另一个消息相结合（例如毗连）。Y 有时起着证明 X 的发送者的身份的作用。

（X、Y）：X 与 Y 的合取和毗连而成的一个消息整体。这里不考虑公钥加密方法，因为它与上面密钥逻辑系统处理相似。

2.3 句法

我们将定义消息的 M_T 语言。在 M_T 中有公式的集合 F_T，诸如 $P \leftrightarrow^{K} Q$ 之类，特别地，时间标记 $T_S \in F_T$

T 包括：实体，P，Q，R，S

公钥： K

Primp：全体一阶原子命题的集合。

M_T 是满足下列构造条件的最小集合：

$M_T \subseteq F_T$

W P，Q，R，S $\in M_T$

$K \in M_T$

Primp $\subset M_T$

$W X_1, X_2, \ldots X_k \in M_T \Rightarrow (X_1, X_2, \ldots X_k) \in M_T$

$W P, K \in T \Rightarrow \{X^P\}_k \in M_T$

$W X, Y, P \in T \Rightarrow <X^P>_Y \in M_T$

$W X \in M_T \Rightarrow$ ‘X’ $\in M_T$

F_T 是满足下列构造条件的最小集合：

$W q \in$ Primp $\Rightarrow q \in F_T$

$W \varphi, \varphi' \in F_T \Rightarrow \neg\varphi, \varphi \wedge \varphi', \neg\varphi' \in F_T$

W P ∈ T， φ ∈ F_T⇒ P believesc φ，P control φ∈ F_T

W P ∈ T，X ∈ M_T⇒ P sees X， P said X, P says X ∈ F_T

W X ∈ T，P， Q∈ T ⇒P # ˣ Q∈F_T

W K ∈ T, P, Q ∈ T ⇒ P $\leftrightarrow^K$Q ∈F_T

W X ∈ M_T ⇒ fresh(X)∈ F_T

W P，K ∈T⇒ Phas K∈ F_T

本文只考虑命题形式的语言，而不考虑带量词的情况。

2.4 公理组

公理均以公理模式的形式表达。

A0：全体一阶命题重言式

A1：Pbelieves φ∧Pbelieves (φ⊃ ϕ) ⊃ Pbelievesϕ

A2：Pbelieves φ ⊃ Pbelieves(Pbelieves (φ))

A3：¬ Pbelieves φ ⊃ Pbelieves (¬ Pbelieves φ)

以上 4 条公理关于实体的信念。

A4：Pbelieves φ ∧ Pbelieves ϕ ≡Pbelieves (φ ∧ ϕ)

A5：如果 P≠S，P $\leftrightarrow^K$Q∧R sees $\{X^S\}_K$⊃ Q said X

A6：如果 P≠S，P $\leftrightarrow^K$Q∧R sees $\{X^S\}_Y$⊃ Q said X

这两条公理是关于消息和它的意义的。

A7：P sees $(X_1,\ldots X_k)$ ⊃ P sees X_i (*1*≤i≤k)

A8：P sees $\{X^Q\}_K$，P has K⊃ P sees X

A9：P sees $<X^Q>_S$ ⊃ P sees X

A10：P sees ‘X’⊃ P sees X

A11：P sees $\{X^Q\}_K$⊃P has K ⊃ Pbelieves(Psees $\{X^Q\}_K$)

这几条公理是关于 Seeing 的。

A12：P said $(X_1,\ldots X_k)$ ⊃ P said X_i (*1*≤i≤k)

A13：P said $<X^Q>_S$ ⊃ P said X

A14：P said 1X’，¬ P sees X⊃ P said X

上述公理中，3said”可用3sees”代替。

A15：Pcontrols φ，P says φ ⊃φ

A16：fresh (X′) ⊃ fresh $(X_{1,}\ldots X_k)$

A17：fresh (X)⊃ fresh ($\{X^Q\}_K$)

A18：fresh (X)⊃ fresh ($<X^Q>_S$)

A19：fresh (X) ⊃ fresh (1X’)

A20：fresh (X)∧P said X ⊃ P says X

A21：$R \leftrightarrow^{k} R' \equiv R' \leftrightarrow^{k} R$，$R \#^{k} R' \equiv R' \#^{k} R$

推理规则有两条：

R1：从 ⊢φ和 ⊢φ ⊃ ϕ推出 ⊢ϕ

R2：从 ⊢φ推出 ⊢Pbelievesφ

上述公理基本上刻画了认证逻辑的许多重要特征和性质。

证明的定义和定理的定义与模态逻辑相似，此处不给出详细定义。

2.5 语义及模型

语义与模型采取类似可能世界的语义与模型。仿照［Abadi, M ., Tuttle, R., 1991］，我们考虑几个参与通信的实体 P_1，P_2，…P_n，有一个特殊的实体 P_e，称为环境(Environment)，它表达通信系统处的网络是否恶意。为讨论方便起见，我们不区分 P_i 是对象语言符号与模型语义符号。给定一个非空集合 π，在给定的时刻 t，每一个实体 P_i 处于特定的状态之中，称为局部状态（local state），记为 $\pi_i(t) \in \pi(t)$，π_e 是环境所处的状态。称〈$\pi_e(t)$〉，$\pi_1(t)$，…，$\pi_n(t)$〉$\in \pi^{n+1}$ 为全局状态（global state），一个路径（run）是全局状态的无穷系列。我们记 r(k)为时刻 k 在路径 r 上的全局状态，$r_i(k)$为相应的 P_i 的局部状态。(r,k)称为点(point)或一个可能世界。当$\pi_i(t)$是 r 中的元素的第 i 个分量时，有$\pi_i(k) = r_i(k)$。

对于每个 P_i 和$\pi_i(t)$，我们认为它包括下列元素

W在与$\pi_i(t)$相对应的时刻 t 之前所完成的动作集合，记为 Action ($\pi_i(t)$)，称为 P_i 的局部历史(local history)，该动作集有下列类型：

——send(m,Q)，P_i 发送消息 m 给 Q，此时 m ∈ buffer ($\pi_Q(t)$)（buffer 见后面的解释）

——receive(P_i, m)，表示 P_i 对消息 m 的接受，m ∈buffer($\pi_i(t)$)

——neukey(K)，表示 P_i 开始拥有密钥 K，K 添加到 P_i 的密钥集中。

W密钥集，它为 P_i 所拥有，记为 keyset($\pi_i(t)$)，t 为某一时刻。

Wbuffer($\pi_i(t)$)集对于 P_i，该集合包含所有已发送给 P_i，但目前时刻 t P_i 尚未发送的消息，约定对于路径的起点 t=*0*的全局状态，buffer($\pi_i(0)$)为空集。

定义 1 设 M 为一个消息，keyset($\pi_i(t)$)简写为 keyset，定义相对于 P_i 的 seen-submsgs(keyset,M),依 M 的形式不同而不同，而 keyset∈P_i 的局部历史。

（*1*）若 M =（X_1,…X_k），则

seen-submsgs (keyset,M)

= {*M*} ∪seen-submsgs (keyset, X_1)…∪seen-submsgs (keyset, X_k)

（*2*）若 M = $\{X^Q\}_S$，k∈keyset，则

seen-submsgs (keyset, M)= {M} ∪seen-submsgs (keyset, X)

（*3*）若 M =< X^Q >$_S$，则

seen-submsgs (keyset, M)= {M} ∪ seen-submsgs (keyset, X)

（*4*）若 M ='X'，则

seen-submsgs (keyset, M)= {M} ∪ seen-submsgs (keyset, X)

直觉上， seen-submsgs (keyset, M)表达消息 M 给解密后的可读内容。

类似地，定义相对于 P_i 的 said-submsgs(keyset, m, M)，m 是 P_i 所接受到的消息的集合，M 是任一消息，那么我们有定义：

定义 2 said-submsgs(keyset, m, M)如下

（*1*）若 $M=(X_1,\ldots,X_k)$，则

said-submsgs(keyset, m, M)= {M} ∪ said-submsgs(keyset, m, X_1) ∪…∪ said-submsgs(keyset, m, X_k)

（*2*）若 $M=\{X^Q\}_K, k\in keyset$, 则

said-submsgs(keyset, m, M)= {M} ∪ said-submsgs(keyset, m, X)

（*3*）若 $M=\{X^Q\}_S$，则 said-submsgs(keyset, m, M)= {M} ∪ said-submsgs(keyset, m, X)

（*4*）若 M = 'X'，且 X ∉seen-submsgs(keyset,M)，则 said-submsgs(keyset, m, M)= {M} ∪ said-submsgs(keyset, m, X)

said-submsgs(keyset, m, M)表示 P_i 收到 M 后返还时所发送信息的内容。

关于语义模型，还必须如下假设：

对任意 P_i 和两个时刻 t，t'，相应地有 keyset，keyset'，则若 t'≤t，则 keyset'⊆ keyset。

send(m,P_i)的发生时间应早于 receive(m, Q)的发生时间。

任 P_i 具有密钥去加密和解密，即

send(M, Q)属于 P 的 t 时刻 local history,且

$\{X^R\}_k$∈said-submsgs(keyset,m,M)

则 $\{X^R\}_k$ ∈ said-submsgs(keyset,m,M)或 K∈ keyset

假定 send(M, Q)属于 P_i 的在 t 时刻局部历史，且 $\{X^R\}_k$ said-submsgs(keyset,m,M)

则 P_i=R 或 $\{X^R\}$ ∈ said-submsgs(keyset,m,M)，同样地对$<X^R>_Y$亦成立。

这个假定保证实体能正确地成为消息源。

一个实体必须知道他所发送的信息的内容。假如 send(M, Q)属于 P_i 的在 t 时刻局部历史，'X' ∈ said-submsgs(keyset,m,M)，那么 X ∈seen-submsgs(keyset,m)

这些要求对于成功的认证协议是必须的。

定义*3* 现在定义可满足关系

设 $\overline{R}$ 的所有 r 的集合，Φ 是解释函数，

Θ：Primp→$\wp$ ({(r,k) $r\in\overline{R}$,k∈ω })

对于 q ∈ Primp，q 在点（r,k）处为真，这样的 q 集合记为 Φ (q)

于是定义φ∈M_T在点（r,k）下的可满足关系（r,k） ⊨φ，如下：

（*1*）（r,k） ⊨φ iff φ∈ (q)，q∈ Primp

（2）（r,k） ⊨φ∧ iff（r,k） ⊨φ和（r,k） ⊨ Φ

（*3*）（r,k） ⊨ ¬ φ　iff 非（r,k） ⊨φ

对下是对各通信行为的原子公式的定义

（*4*）（r,k） ⊨P_i sees X iff 对于消息 M 和对于点（r,k），有

——receive(M)属于 P_i 的局部历史；

——X∈ Seen-submsgs(keyset,M)，keyset 属于 P_i 的 keyset.

（*5*）（r,k） ⊨P_i said X,iff

对于某些 M，在点（r,k）处，存在点（r,k'），有 k' ≤k

——P_i 完成动作 send（M,Q）

——X∈said-submsgs（keyset，m,M）

keyset 属于 P_i 的局部历史，m 是 P_i 所接受的消息集合。

（*6*）（r,k） ⊨P_i says X,与同(*5*)一样定义，只是*0d*k' *d*k

（*7*）（r,k） ⊨P controlφ iff，（r,k'） ⊨P_i says φ⇒（r,k'） ⊨φ，对于所有 k'≥ 0

（*8*）（r,k） ⊨fresh(X) iff X⊄S ubmsgs（M（r））

（*9*）（r,k） ⊨ P $\leftrightarrow$ ^{K}Q iff 对于所有 k'，（r,k'） ⊨R said $\{X^S\}_k$⇒(r,k') ⊨R sees $\{X^S\}_k$ 或 R ∈ {P,Q}

（*10*）（r,k）⊨P #^{x}Q iff 对于所有 k'，（r,k'）⊨R said $\{X^S\}_Y$ ⇒（r,k'）⊨R said$\langle Y^S\rangle_X$ 或者 R ∈ {P,Q}。

至于 beliefs 的可满足关系的定义，先引进几个概念：

W在 t=*0* 时刻 P_i 的信念集定义为相应时刻 P_i 的路径集 G_i ，其中对于任意一个路径 r，这些信念都为真。

W对于 P_i 的局部状态π_i(t)，用 hide(π_i(t))记 P_i 在状态π_i(t)时他不能解读的消息。定义关系$\sim_i$，对于任意（r,k），（r',k'），（r,k）$\sim_i$（r',k'） iff r' ∈G_i ，且 hide（π_i(k)）= hide（π_i'(k')），与π_i(k)，π_i'(k')相应的全局状态π(k)∈r 和π'(k')∈r'，为方便起见，此式亦可写为 hide（π_i(k)）= hide（r_i'(k')），之所以引进这个定义，主要是要刻划 P_i 的信念集以及信念集如何在另一个可能世界或点中同样为真，这与模态逻辑定义〃必然〃相类似，沿着这个思路，我们给出 Beliefs 的可满足关系，信念在具有可达关系的另一个可能世界中为真。

(*11*)（r,k） ⊨P_i believes φ　iff

（r',k'） ⊨φ，对于所有（r',k'），使得（r,k）$\sim_i$（r',k'）

我们引用文[A badi, Tuttol, 1991]的结论：

定理*1*　公理组的每个公理模式在给定模型下是有效的。

同时该文也证明了公理系统并不是完全的。

3、对于模型的修正

模型在很大程度上说明了我们对认证协议所具有的特性。不过有两点尚待改进的地方：

（*1*）在公理系统里，⊨P_i believes φ⊃φ不是定理，因而作相应的语义模型中下不应为真。但是由于关系（r,k）$\sim_i$（r',k'）满足自反性，即（r,k）$\sim_i$（r,k），因而 ⊨P_i believes φ⊃φ，而不管（r,k）取何值，这意味着 ⊨P_i believes φ⇒ ⊨φ，但是这并不符合我们对协议逻辑的过

程直觉，尤其不适合 P_i believes $P \leftrightarrow^{K} Q$ 的场合[Abadi, M., Tuttle, 1991]这表明用$\sim_i$比拟可通达关系并不恰当。

（2）设$\pi_i(t)$，$\pi_i(t')$为 P_i 在 r 上的两个状态，可以定义***d***关系满足$\pi_i(t) \geq \pi_i(t') \Leftrightarrow t \geq t'$因当 $t \geq t'$时，$keyset(\pi_i(t)) \subseteq keyset(\pi_i(t'))$。由于 $hide(\pi_i(t)) = hide(\pi_i(t'))$，一方面，由于 Newkey 集合的包含关系从而使后一时刻用***K***解密的句子增加因而使 $hide(\pi_i(t))$的集合的基数变小，而上述有关 hide 的表达则正好相反。因此，对$\sim_i$关系用 hide 运算来刻划是不合情理的。

为了更符合认证协议的实际，我们只修改有关 Belivefs 的部分。

定义*4* 对于实体 P_i，$\varphi \in M_T$，定义（r,k）处的 belivefs 可满足关系为（r,k）$\vdash P_i$ believes φ iff 对于所有满足关系＜（r,k），（r',k'）＞$\in$R(i)的（r',k'），有（r',k'）$\vdash\varphi$，其中 R(i)称为 P_i 的可达关系，具有下列性质：

（***1***）R(i)是传递关系

（2）〈 (r,k) （r',k')〉$\in$R(i)$\Rightarrow$hide(r_i (k))= hide(r'(k'))

（***1***）是为证明***A2***准备的，这与模态逻辑 S***4***相类似；（2）保留了前面定义的直觉，即信念不能对不能解读的信息发生关联。同时，在公理组中，利用（2）可以帮助验证公理系统的有效性。

定理2 对于任意(r,k）有(r,k) $\vdash P_i$ sees $\{X^Q\}_K \wedge P_i$ has K $\supset$P believes(P_i $\{X^Q\}_K$)

证明：(r,k) $\vdash P_i$ sees $\{X^Q\}_K \wedge P_i$ has K$\Rightarrow$(r,k) $\vdash P_i$ sees $\{X^Q\}_K$，并且(r,k)$\Leftarrow$ P_i hasK。

$\Rightarrow$ 存在 M，有 receive(M) 属于 (r,k) 时 P_i 的局部历史，且 X $\in$seen-submsgs(Keyset,X) $\cup$ $\{X^Q\}_k$。

由 R_i （(r,k),(r',k')）的性质（2）知，存在 M，使 receive(M)出现在（r',k'）时 P_i 的局部历史中，且 X $\in$ sees-submsgs（Keyset,X）$\cup$ $\{X^Q\}_K$，故有

(r', k') $\vdash P_i$ sees $\{X^Q\}_K$

依定义因而原式成立。

有了定理***2***，那么我们可以验证，***A1***，***A2***，***A3***，***A4***，***A11***有关 Beliefs 的公理，***A11***由定理***2***所证明，***A1***，***A2***，***A3***，***A4***的验证仿对应于模态逻辑 S4 的方法。其余公理的验证与论文[Abadi, m., Tutter, R., 1991]相同。因此，我们有

定理*3* 公理***A1~A22***在修改后的模型中是有效的。

此定理表明我们修改后的语义模型亦具有有效性，但是我们的模型更具有实践上的合理性。

4、结论

对模型的争论与修正大都集中在对于 Beliefs 的可满足关系和可通达关系的刻画上，通常的思路借用 Kripke 型语义模型的定义方式，但如何保证刻画既直观又严密是值得尝试的工作，至于语义刻画是否有更好的性质如完全性等，将是进一步努力的方向。

参考文献

[1] Abadi, M., Tuttle, R., 1991, A semantics for a logic of Authentication (Extended Annual), in *proceedings of the tenth Annual ACM symposium on principles of pistriblted computing,* PP201-216.

[2] Agray, N, Van der Hoek, E. de Vink ,2002, on BAN logics for industrial security protocols in *CEEMAS 2001, LNAI2296*, PP26-36, Springer-Verlag.

[3] [BAN] Burrows, M., Abadi, M., Needham, R., 1990,. A logic of Authentication, *ACM Translations on Computer systems,* Vol.8 PP18-36.

[4] 白硕，隋立颖，陈庆锋，付岩，庄超，安全协议的验证逻辑，2000 软件学报，11（2），PP213-221。

[5] [GNY] Gong, L., Needham, R., Yahalom, R., Reasoning about Belief in cryptographic protocol Analysis, 1990, *Proc. IEEE symp. on Research in security and privacy,* PP234-348.

[6] Gunnar, H., GSM Network: Protocols, Terminology, and Implementations, 1999, Artech House.

On the Refinement for the Semantics model of BAN logic

FEI Ding-zhou[1] DENG Da-qiang[1]

(Institution for logic and Cognition, Zhongshan University, Guangzhou 510275)

Abstract: This paper focuses on the remedy for the model of BAN, especially the part of beliefs, in addition to describing of the original BAN logic version. We think this refinement in semantics of BAN can give move reasonable expression than the authors and other discussions, for example, by GNY.

Keywords: Authentication logic； BAN logic；Semantics model

收稿日期：2003 年 8 月

作者简介:

费定舟，博士生，研究方向为认知逻辑和 Agent 理论

邓达强，博士，研究方向为数据库和程序设计

本文写作得到鞠实儿教授的帮助，特此致谢