一种 BAN- 逻辑的修正 [1]

郑 东 王常杰 王育民
(西安电子科技大学 105 室 西安 710071)

摘 要 本文指出了 BAN- 逻辑推理中存在的逻辑错误，提出了一种改进的 BAN- 逻辑，它具有精确的语义定义和正确的推理规则，当协议的初始条件正确时，逻辑推理的结论是正确的.
关键词 认证协议， BAN- 逻辑
中图号 TN918

1 引 言

Burrows, Abadi 及 Needham 在 1989[1] 年提出了一种密码协议的安全性分析方法——BAN-逻辑，该逻辑成功地发现了许多著名协议中存在的漏洞，但其最大缺点是：它证明安全的协议可能是不安全的 (如对并行攻击的无效性) . 导致这种结果的主要原因是 BAN-逻辑中含有一些模糊的 (非形式的) 假设描述. 之后，一些作者给出了进一步改进 [2-8] ，但这些改进仍然没有克服上述缺点，其给出的逻辑语义仍然是非形式的. BAN-逻辑的不足可归纳如下： (1) 逻辑不够严密 (如用共享密钥加密的数据的来源判断)； (2) 逻辑语义不清楚 (如主体能够识别消息的含义是模糊的) . 本文试图利用逻辑公式的真值使得逻辑语义精确化. 同时，给出了严格的逻辑推理规则. 我们在第一部分，通过 BAN-逻辑对一个实例的错误分析，指出 BAN-逻辑中语义的模糊性及错误的推理规则；第 2 节给出了新的推理规则；第 3 节给出了一个实例分析.

2 BAN 中的逻辑错误

2.1 BAN-逻辑

在 BAN-逻辑中，若 P Sees $\{X\}_{K_{PQ}}$ 且 P believes $P \overset{K_{PQ}}{\longleftrightarrow} Q$, 则 P believes Q Said X , 但实际上，上述规则隐含这样的假设： Q Said $\{X\}_{K_{PQ}}$ ，这个假设可能不成立. P 仅有共享密钥 K_{PQ} 是不能相信消息 $\{X\}_{K_{PQ}}$ 来源于 Q(可能 P 发送过消息 $\{X\}_{K_{PQ}}$ ，即 P Said $\{X\}_{K_{PQ}}$) . 下列协议的证明及对其成功的并行攻击说明这个事实：

图 1 的说明：在询问 -应答协议中 (图 1)， B 向 A 发出随机数 R_B(询问)，然后， A 向 B 发送 $\{R_B\}_{K_{AB}}$(应答)， K_{AB} 是 A 与 B 的共享密钥；

图 2 并行攻击的说明： Z 为了冒充 A 而获得 B 的认证，当收到 B 发送的信息 R_B 后，又冒充 A 并行地发起了一次协议运行，使用的还是一次性的随机数 R_B ， B 收到后，响应发出 $\{R_B\}_{K_{AB}}$, Z 收到响应后，把其应用到前面的协议运行，从而获得 B 的认证. 但由 BAN-逻辑可以证明， B believes $A| \approx R_B$(B believes that A has recently said X) . 协议的理想化如下：

[1] 1998-11-16 收到， 1999-06-28 定稿
国家自然科学基金 (6983005) 及国防科技保密通信重点实验室基金资助

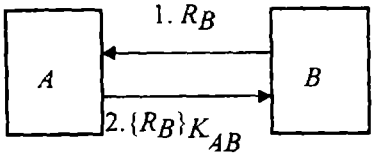

图 1 询问－应答协议

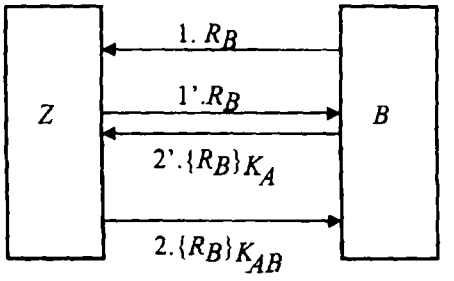

图 2 并行攻击

(1) $A \triangleleft R_B$ 。

(2) $B \triangleleft \{R_B\}_{K_{AB}}$ 。

(3) B believes $\#R_B$ 。

(4) B believes $\rho(R_B)$ 。

(5) B believes $A \overset{K_{AB}}{\longleftrightarrow} B$ 。

认证目标： B believes $A| \approx R_B$(B believes that A has recently said X) 。

BAN-逻辑有如下规则：

$A_1 : \frac{P \triangleleft \{X\}_K, P| \equiv P \overset{K}{\longleftrightarrow} Q, P| \equiv \rho(X)}{P| \equiv Q| \sim X, P| \equiv Q| \sim K, P| \equiv Q| \sim \{X\}_K}$ 。

$A2 : \frac{P| \equiv Q| \sim X, P| \equiv \#X}{P| \equiv Q| \approx X}$ 。

由 $A1$, (2), (4), (5) 及 $A2$ 可以得到 B believes $A| \approx R_B$ 。但图 2 的并行攻击是成功的。即 BAN-逻辑对并行攻击是无能为力的。BAN-逻辑的这种失败是由于不正确的逻辑规则所导致。在规则 $A1$ 中，隐含着一个假设条件： $P| \equiv Q| \sim \{X\}_K$ ，并没有给出此条件的正确性验证，这是导致逻辑证明失败的原因之一。仅有共享密钥 K_{PQ} 是不能判断用 K_{PQ} 加密的消息是由 P 生成的还是 Q 生成的。

2.2 消息新鲜性的判断规则

在 BAN-逻辑中，对消息新鲜性的判断有如下规则：

P sees $F_{K_{PQ}}(N, X_1, \cdots, X_n)$ 且 P Believes $\#N$ ，则 P believes $\#(N, X_1, \cdots, X_n)$ ，而认证协议中，最需要的是某个 X_i 是否是新鲜的，由于 $F_{K_{PQ}}(N, X1, \cdots, X_n)$ 的定义非常模糊，很容易错误得出一些结论 (如 M. Wenbo[4] ，就是错误地假设了 $F_{K_{PQ}}(N, X_1, \cdots, X_n) = (\{K, \cdots\}_{K_{PQ}}, \{\cdots\}_K)$ 而得出错误的结论)。本文给出了下列推理规则：设 F 是一对一函数，定义 $F_{K_{PQ}}(X1, \cdots, X_n) \equiv \{F(X1, \cdots, X_n)\}_{K_{PQ}}$(如 $F(X_1, \cdots, X_n) = (X_1, \cdots, X_n)$) ，若 P sees $F_{K_{PQ}}(X_1, \cdots, X_n)$ 且 P believes $\#X_i$ ，则 P believes $\#X_j$, $1 \le j \le n$ 。

3 新的推理规则

3.1 消息的定义

在密码协议的实施过程中，交换的消息是通过对最小单位的子消息进行连接，加密得到的，这种最小单位的消息称做原子消息，我们有以下 4 类原子消息：

(1) 密钥 (key)： (主体的公开密钥 P key ，私钥 S key ，对称密钥 key ，密钥是用于对消息进行加密的消息，我们总是假设加密是完备加密，即要得到加密消息的明文，必须通过

用正确的密钥对消息解密；

(2) 主体名称 (principal)：实施协议的主体名称 (如：A, B, S)；

(3) 一次性随机数 (nonce)：一次性随机数是用来保证一个消息是最新生成的；

(4) 数据 (data)：数据消息不能控制通信的规则，仅是主体之间要通信的消息。

设 $l\omega$ 是原子消息空间，则基于 $l\omega$ 上的所有消息的集合 M 归纳定义如下：

(a) $a \in \omega$，则，$a \in M$。(b) 若 $m_1 \in M$，且 $m_2 \in M$，则 $m_1 \cdot m_2 \in M$。(c) 若 $m \in M$ 且 $k \in KEY$, $KEY \subset M$ 是密钥集合，则 $\{m\}_k \in M$，即一个消息被正确加密后，成为新的消息，同时，如果 k^{-1} 是 k 的逆密钥，则 $\{\{m\}_k\}_{k^{-1}} = m$。(d) 完备性 生成消息 $\{m\}_k$ 的唯一方法是由密钥 k 对消息 m 进行加密运算得到，即如果 $\{m\}_k = \{m'\}_{k'}$，则 $m = m'$，且 $k = k'$。

3.2 对消息的基本断言 (或基本陈述)

$\#X$：表示 "消息 X 是新鲜的"；

P received X: P 收到 X；

P comprehend $X(P| \equiv \rho(X)$: P 能够识别接收的消息 X；

P Sees $X(P \triangleleft X)$：P 看见消息 X；

P once-Said $X(P| \sim X)$：P 曾经说过 X；

P Say $X(P| \approx X)$：P 最近说过 X；

P possess $X(P \ni X)$：P 拥有消息 X。

公式的定义 (公式由以下递归定义)

(1) 一个基本断言是一个公式；

(2) 若 φ 是公式，则 P believes φ 是公式；

(3) 若 φ、ϕ 是公式，则 $\phi \wedge \varphi, \phi \to \varphi$ 是公式 ("$\wedge$" 表示逻辑 "与"，"$\to$" 表示逻辑蕴涵)；

(4) 若 φ 是公式，P Controls φ 是公式；

(5) 若 $K \in Key$，则 P possesses K 是公式，主体 P 拥有密钥 K；

(6) 若 $K \in Key$，$P \xleftrightarrow{K} Q$ 是公式 (K 是 P 与 Q 秘密密钥，此密钥一般在协议的说明中给出)(不包括要交换的会话密钥)。

3.3 永真公式集合 Γ

(1) $\forall P \in$ Principal, P possesses $K_R \equiv T$，即每个主体拥有其它主体的公开密钥永真；

(2) $\forall P \in$ principal, P possesses $K_P^{-1} \equiv T$，即每个主体拥有自己的私钥永真；

(3) 若 K_{PQ} 是 P 与 Q 的对称密钥 (初始条件)，则 $P \xleftrightarrow{K} Q$ 永真，P possesses $K_{PQ} \equiv T$, Q possesses $K_{pq} \equiv T$，即每个主体拥有自己与其它主体的对称密钥永真；

(4) $\forall P \in$ Principal, P believed $\#N_a \equiv T$；("P 相信自己生成的随机数是新鲜的" 永真，我们假设主体总是能够正确判断自己生成的一次性随机数)。

基本规则：

(1) 若 $\varphi \in \Gamma$，则 P believed $\varphi = T$；

(2) P received $X = T$，则 $P \triangleleft X = T$；

(3) $\phi \wedge \varphi = T \Leftrightarrow \phi = T \wedge \varphi = T$；

(4) 若 $\phi \Leftrightarrow \varphi$，则 $P| \equiv (\phi \to \varphi) = T$；($\phi \Rightarrow \varphi$ 表示 "$\phi \to \varphi \equiv T$")，$P| \equiv (\phi \to \varphi) \Rightarrow P| \equiv \phi \to P| \equiv \varphi$；

(5) $P| \equiv \phi \wedge \varphi \Leftrightarrow P| \equiv \phi \wedge P| \equiv P$;

Seeing

(6) $P \triangleleft (X_1, \cdots, X_n) \Rightarrow P \triangleleft X_i,\ i = 1, \cdots, n$; (若 $P \triangleleft (X_1, \cdots, X_n) = T$, 则 $P \triangleleft X_i = T$) ;

Freshness

(7) $P| \equiv \#X \Rightarrow P| \equiv (X_1, \cdots, X_i, \cdots, X_n),\ i = 1, \cdots, n$;

Said and says

(8) $P| \equiv Q| \sim (X_1, \cdots, X_n) \Rightarrow P| \equiv Q| \sim X_i,\ i = 1, \cdots, n$;

(9) $P| \equiv Q| \approx (X_1, \cdots, X_n) \Rightarrow P| \equiv Q| \approx X_i,\ i = 1, \cdots, n$;

Recognizing

(10) $P| \equiv \rho(X_1) \wedge \cdots \wedge P| \equiv \rho(X_n) \Rightarrow P| \equiv \rho(X_1, \cdots, X_n)$;

Nonce Verification

(11) $P| \equiv Q| \sim X \wedge P| \equiv \#X \Rightarrow P| \equiv Q| \approx X$;

Symmetric Enciphering

(12) 若 F 是消息的一对一函数 (如消息的级连运算 $F = (X_1 X_2 \cdots X_n)$, 则 $P \triangleleft F_{K_{PQ}}(s_Q, X_1 \cdots X_n) \Rightarrow P| \equiv Q| \sim (X_1 \cdots X_n)$; (即若 $P \triangleleft F_{K_{PQ}}(s_Q, X_1 \cdots X_n) = T$, 则 $P| \equiv Q| \sim (X_1 \cdots X_n) = T$(其中 $F_{K_{PQ}}(s_Q, X_1 \cdots X_n) = \{F(s_Q, X_1 \cdots X_n)\}_{K_{PQ}}$, S_q 是消息来源认证符, 表示此消息是 Q 说过的, 在协议理想化时, 要说明是否有消息来源认证符) ;

(13) $P \triangleleft F_{K_{PQ}}(s_Q, N_P, X_1 \cdots X_n) \wedge P| \equiv \#N_P \Rightarrow P| \equiv X_i, 1 \le i \le n)$, 由 (11) 和 (12) 得 $P \triangleleft F_{K_{PQ}}(s_Q, N_P, X_1 \cdots X_n) \wedge P| \equiv \#N_P \Rightarrow P| \equiv Q| \approx X_i, 1 \le i \le n)$;

(14) $P| \equiv \rho(X) \wedge P$ possesses $K \Rightarrow P| \equiv \rho(\{X\}_K)$;

(15) $P| \equiv Q| \approx \{X\}_K \wedge P$ possesses $K \Rightarrow P| \equiv Q| \approx X$;

Asymmetric Enciphering

(16) P possesses $K^{-1} \wedge P \triangleleft \{X\}_K \Rightarrow P \triangleleft X$, 这里, K^{-1} 是公开密钥 K 的解密密钥, BAN 中类似的规则为 $\frac{P \text{ possesses } K^{-1}, P \text{ sees } \{X\}_K}{P \text{ sees } X}$;

(17) $P| \equiv \rho(X) \wedge P| \equiv \xrightarrow{K} P \Rightarrow P| \equiv \rho(\{X\}_K)$, 这里 $\xrightarrow{K} P$ 表示 K 是 P 的公开密钥;

(18) $P \triangleleft \{X\}_{K^{-1}} \wedge P$ possess $\xrightarrow{K} Q \Rightarrow P \triangleleft X$;

(19) $P \triangleleft \{X\}_{K^{-1}} \wedge P$ possess $\xrightarrow{K} Q \wedge P| \equiv \rho(X) \Rightarrow P| \equiv Q| \sim X \wedge P| \equiv Q| \sim \{X\}_{K^{-1}}$;

(20) $P| \equiv \#X \wedge P$ possess $\xrightarrow{K} Q \Rightarrow P| \equiv \#\{X\}_K$;

(21) $P| \equiv \rho(X) \wedge P$ possess $\xrightarrow{K} Q \Rightarrow P| \equiv \rho(\{X\}_{K^{-1}})$;

(22) $P| \equiv Q| \approx \{X\}_{K^{-1}} \wedge P$ possess $\xrightarrow{K} Q \Rightarrow P| \equiv Q| \approx X$.

上述规则中, 没包含的 BAN 规则:

在 BAN 逻辑中, P Sees $\{X\}_{K_{PQ}}$ 且 P believes $P \overset{K_{PQ}}{\longleftrightarrow} Q$, 则 P believes Q Said X , 但实际上, 并没有排除 P Said X , 因此, 上述推理需满足条件 Q Said $\{X\}_{K_{PQ}} = T$.

3.4 与 BAN-逻辑的区别

(1) 对公式给出了真值;

(2) 对 BAN 中的公式 P Sees $\{X^Q\}_{K_{PQ}}$ 给出了真值的判断 (规则 (10), (11)) , 避免了在 BAN 中容易出现判断错误的可能性) ;

(3) 对 nonce 的规则进行了改进 (规则 (11)) ;

(4) 对捆绑加密 $F_{K_{PQ}}(N_P, X_1, \cdots, X_n)$ 给出了精确的说明。

4 例　子

例 1　对询问-应答协议 (图 1) 的理想化及逻辑分析：

(1) A received $R_B = T$；　(2) B received $\{R_B\}_{K_{AB}} = T$；　(3) A possess $K_{AB} = T$；　(4) B possess $K_{AB} = T$；　(5) $B| \equiv \#R_B = T$；　(6) $B| \equiv \rho(R_B) = T$；　(7) $A| \equiv A \overset{K_{AB}}{\longleftrightarrow} B = T$；　(8) $B| \equiv A \overset{K_{AB}}{\longleftrightarrow} B = T$.

认证目标：　$B| \equiv A| \approx R_B = T$(“ B 相信 A 最近说过 R_B ” 取值为真).

由 (1), ⋯, (8) 及推理规则 (11)：我们要推出 $B| \equiv A| \approx R_B = T$，则需有 $B| \equiv A| \sim \{R_B\}_{K_{AB}} = T$ 及 $B| \equiv \#R_B = T$；再由规则 (12) 我们得到：对用共享密钥 K_{AB} 加密的消息 $\{\cdots R_B\}_{K_{AB}}$，接收者 B 通过消息来源认证符认证消息 $\{\cdots R_B\}_{K_{AB}}$ 是否来源于 A，而消息 $\{R_B\}_{K_{AB}}$ 中，不含消息认证符，说明 B 难以相信 “ A 曾经说过消息 $\{R_B\}_{K_{AB}}$ ”，即我们不能得出 $B| \equiv A| \sim \{R_B\}_{K_{AB}} = T$．由此，我们可以得出，此协议没有达到认证目标 $B| \equiv A| \approx R_B = T$.

例 2　Woo-Lam 认证协议

Message1 $A \to B : A$．Message2 $B \to A : N_b$．Message3 $A \to B : \{N_b\}_{K_{as}}$．Message4 $B \to S : A, B, \{N_b\}_{K_{as}}$．Message5 $S \to B : \{A, N_b\}_{K_{bs}}$.

真值公式如下：

(1) B received $A = T$；　(2) A received $N_b = T$；　(3) B received $\{N_b\}_{K_{as}} = T$；　(4) S received $A, B, \{N_b\}_{K_{as}} = T$；　(5) B received $\{A, N_b\}_{K_{as}} = T$；　(6) A possess $K_{as} = T$；　(7) B possess $K_{bs} = T$；　(8) $B| \equiv \#R_B = T$；　(9) $B| \equiv \rho(R_B) = T$；　(10) $A| \equiv A \overset{K_{as}}{\longleftrightarrow} S = T$；　(11) $B| \equiv B \overset{K_{bs}}{\longleftrightarrow} S = T$.

认证目标：　$S| \equiv B| \approx \{A, B, \{N_b\}_{K_{as}}\}$, $B| \equiv S| \sim \{A, N_b\}_{K_{bs}} = T$.

由基本规则 (11)(Nonce Verification) 得知，若 $S| \equiv B| \approx \{A, B, \{N_b\}_{K_{as}}\} = T$, 则应有 P 相信的新鲜子 N_S，而此协议中，S 不产生新鲜子，因此，我们无法得出 $S| \equiv B| \approx \{A, B, \{N_b\}_{K_{as}} = T$．对 Woo-Lam 协议的攻击 1 证实了这一点.

若要得出 $B| \equiv S| \approx \{A, N_b\}_{K_{bs}} = T$，则需 $B| \equiv S| \sim \{A, N_b\}_{K_{bs}} = T$ 及 $B| \equiv \#N_b = T$，再由基本规则 (12) 得出，对由共享密钥 K_{bs} 加密的消息，接收者要通过消息来源认证符判断加密的消息是否来源于 S，在消息 $\{A, N_b\}_{K_{bs}}$ 中没有消息来源认证符，B 无法相信 $\{A, N_b\}_{K_{bs}}$ 一定来源于 S，我们得不到 $B| \equiv S| \sim \{A, N_b\}_{K_{bs}} = T$．如下的攻击 2 说明了这一点.

攻击 1

(1.1) $I(A) \to B : A$,　(1.2) $B \to I(A) : N_b$;　(2.1) $B \to I(C) : B$,　(2.2) $I(C) \to B : A, N_b$,　(2.3) $B \to I(C) : \{A, N_b\}_{K_{bs}}$;　(1.3) $I(A) \to B : X$,　(1.4) $B \to I(S) : A, B, X$,　(1.5) $I(S) \to B : \{A, N_b\}_{K_{bs}}$.

攻击 2

(1.1) $I(A) \to B : A$;　(1.2) $B \to I(A) : N_b$;　(1.3) $I(A) \to B : X$;　(1.4) $B \to S : A, B.X$;　(2.1) $A \to I(B) : A$;　(2.2) $I(B) \to A : N_b$,　(2.3) $A \to I(B) : \{N_b\}_{K_{as}}$;　(3.1) $I(B) \to S : A, B\{N_b\}_{K_{as}}$,　(3.2) $S \to I(B) : \{A, N_b\}_{K_{bs}}$;　(1.5) $I(S) \to B : \{A, N_b\}_{K_{bs}}$.　(在上述攻击中，$X$ 表示任意消息)

5 结 论

BAN-逻辑能够成功地发现一些密码协议可能存在的攻击，但由于语义模糊及逻辑推理不严密，使得可能把实际不安全的协议证明是安全的．我们通过对逻辑语句给出真值的定义，使得语义精确化，推理是基于数理逻辑的真值推理，因此，避免了 BAN-逻辑存在的一些缺陷．当协议的初始条件正确给定时，推出的结论是正确的．

参 考 文 献

[1] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990, 8(1): 18–36.

[2] Boyd C, Mao W. On a limitations of BAN logic. In Lecture Notes in Computer Science 765, Berlin: Springer-Verlag, 1993, 240–247.

[3] Nessett D M. A Critique of Burrows, Abadi and Needham logic. Operating Systems Review, 1990, 24(2): 35–38.

[4] Li Gong, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. In Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California: 1990, 234–248.

[5] Abadi M, Tuttle M. A semantics for a logic of authentication. In Proceedings of the Tenth ACM Symposium on Principles of Distributed Computing, Sanantonio, Texas: ACM Press, August 1991, 201–216.

[6] Syverson P, Van Oorschot P C. On unifying some cryptographic protocol logics. In Proceedings of 1994 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Okland California: 1994, 165–177.

[7] 田建波，徐胜波，王育民．一种改进的认证逻辑．电子学报，1998, 26(7): 175–177.

[8] 郑东，田建波、王育民．关于 BAN-逻辑的注记．China Crypt'98, 北京：科学出版社，1998, 123–125.

A MODIFIED BAN-LOGIC

Zheng Dong Wang Changjie Wang Yumin

(*Xidian University, Xi'an* 710071)

Abstract This paper points out some flaws in BAN-logic, and presents a modified version of the BAN-logic, which has a sound semantics and correct loigc rules. It is concluded that, if the initial condition is right, the result from this logic is right as well.

Key words Authentication protocol, BAN-logic

郑 东： 男，1964 年出生，博士，研究方向：通信保密与网络安全，主要从事认证协议的安全性分析与伪随机性的研究．

王常杰： 男，1974 出生，博士生，研究方向：通信保密与网络安全．

王育民： 男，1936 年出生，教授，博士生导师，主要从事信息安全与编码理论研究．