关于 BAN 逻辑扩展的注记 [1]

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

摘 要 本文指出了 W.Mao(1995) 对其协议 (1) 的证明中存在的错误，并对其在协议理想化过程中提出的 $N-u$ 规则作了探讨，指出其扩展 $N-u$ 的三条规则的缺陷，并作了改进，最后，给出一个例子说明 $N-u$ 规则的应用.

关键词 认证协议，BAN 逻辑
中图号 TN918

1 引 言

自 Burrows, Abadi 和 Needham 在文献 [1] 中提出关于分析认证协议的形式逻辑以来，已有许多作者指出了它的一些弱点并作了改进，见文献 [2,3]. Mao 在文献 [4] 中对协议的理想化作了讨论，提出了协议理想化规则. 但这两方面的工作仍然不是令人满意的. 由于没有精确的语义定义，使得证明容易出错，下面的例子就说明了这一点. 在文献 [4] 中，虽然提出了协议理想化的三条规则，但还不够完善，本文对这种规则作了进一步的修改.

2 关于文献 [4] 中的一个 BAN 逻辑证明的商榷

我们先看下面的协议 (参看图 1):

$$\left.\begin{array}{l}(1)\ A \to B : A, \{N_a, A\}_{K_{as}}, \\ (2)\ B \to S : A, B, \{N_a, A\}_{K_{as}}, \{N_b, B\}_{K_{bs}}, \\ (3)\ S \to A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}}, \\ (4)\ A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}.\end{array}\right\} \quad (1)$$

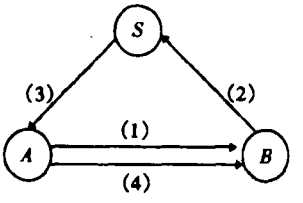

图 1

Mao 在文献 [4] 中用 BAN-like 逻辑证明该协议能够使得

$$A \quad \text{believes} \quad A \overset{K_{ab}}{\longleftrightarrow} B,$$

[1] 1997-10-24 收到，1999-03-01 定稿
国家自然科学基金资助课题 (69683005)

但是这个结论是不成立的，协议 (1′) 式 (文献 [4] 中的攻击 3) 给出上述协议是易被重放攻击的.

$$\left.\begin{array}{l}(1)\ A \to C_b : A, \{N_a, A\}_{K_{as}},\\ (2)\ C_a \to S : C, A, \{N_c, C\}_{K_{cs}}, \{N_a, A\}_{K_{as}},\\ (3)\ S \to C : \{K_{ca}, A\}_{K_{cs}}, \{N_c, N_a, \{K_{ca}, C, N_a\}_{K_{as}}\}_{K_{ca}},\\ (3')\ C_s \to A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_c\cdot\}_{K_{ab}},\\ (4)\ A \to C_b : \cdots, \{N_c\}_{K_{ab}}.\end{array}\right\} \quad (1')$$

其中 C_x 表示 C 伪装 X， (1′) 式中的 (3′) 中的 K_{ab} 是以前被泄露的密钥.

文献 [4] 中认为这种证明失败是由于没有标准的理想化方法导致的. 本文认为导致这种结果的原因是由于证明的错误引起的.

文献 [4] 中的证明是假设下列初始条件成立:

(1) A believes $A \overset{K_{ab}}{\longleftrightarrow} S$,

(2) A believes S controls $(A \overset{K_{ab}}{\longleftrightarrow} B)$

(3) A believes fresh (N_a),

(4) A received F_{Kas} $(A \overset{K_{ab}}{\longleftrightarrow} B, N_a, \cdots)^S$,

(5) A believes A sees $(N_a, \cdots)$,

(6) A believes A sees $(A \overset{K_{ab}}{\longleftrightarrow} B)$,

在上述假设中， $F_{K_{as}}(A \overset{K_{ab}}{\longleftrightarrow} B, N_a, \cdots)^S = \{K_{ab}, B\}_{K_{as}}, \{N_a, \cdots\}_{K_{ab}}$ ，但文献 [4] 对协议证明时，错误地把 $F_{K_{as}}(\cdots)^S$ 与 $\{\cdots\}_{K_{as}}$ 等同起来，这样就导致证明的失败. 事实上，在 Mao 的协议 (1) 中，只有 A received $\{K_{ab}, B\}_{K_{as}}$, $\{N_a, \cdots\}_{K_{ab}}$ 由此按照 BAN 逻辑推导得不到： A believe S said $A \overset{K_{ab}}{\longleftrightarrow} B, Na, \cdots)$ ，也得不到 A believes fresh $(A \overset{K_{ab}}{\longleftrightarrow} B)$.

3 关于 $N-u$ 的扩展

Mao 在文献 [4] 中指出协议的理想化过程在 BAN 逻辑证明中起着重要的作用，提出了在协议理想化时， N(freshness identifier) 的扩展方法，即用 $N-u$ 代替 N 的方法. N 是按下列规则递归定义的主体名的集合:

记号： $M \Rightarrow M'$: 表示协议理想化过程中，将协议中的所有 M 用 M' 代替.

sort: 协议中所有主体组成的集合.

规则如下:

(Ⅰ) 如果 $P \overset{K}{\longleftrightarrow} Q \wedge P \overset{k}{\text{said}}_A (N-u, R)$, 则 $N-u \Rightarrow N-(u \cup \{R\})$;

(Ⅱ) 如果 $P \overset{K}{\longleftrightarrow} Q \wedge P \overset{k}{\text{said}}_c N-u$, 则 $N-u \Rightarrow N-(u \cup \{Q\})$;

(Ⅲ) 如果 $P \overset{K}{\longleftrightarrow} Q \wedge P \overset{k}{\text{sees}}_A (N-u, R)$, 则 $x \to P : \cdots, \{\cdots, N-u, \cdots\}_{K,\ldots} \Rightarrow x \to P : \cdots, \{\cdots, N-(u \cup \{R, Q\}, \cdots\}_k, \cdots$.

Mao 指出，若按这三种规则，主体 B 不能属于 $N-u$，则发送 N 的主体 A 就不能了解 B 的“最近状况”，即不能了解这次协议实施中 B 的状况．该结论对分析一个协议的安全性的确是有意义的 (虽然未被证明)，但本文认为由上述规则扩展的 $N-u$ 规则并不能包含 N 的发送者可了解的所有主体．我们看下面 Mao 的协议 (2)：

$$\left.\begin{array}{l}(1)\ A \to B : A, \{N_a, A\}_{K_{as}};\\ (2)\ B \to S : A, B, \{N_a, A\}_{K_{as}}, \{N_b, B\}_{K_{bs}};\\ (3)\ S \to A : \{K_{ab}, N_a\}_{K_{as}}; \{B, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}};\\ (4)\ A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}.\end{array}\right\} \tag{2}$$

此协议是抗文献 [4] 中的重放攻击 (3) 的，且易证明：

$$A \quad \text{believes} \quad A \overset{K_{ab}}{\longleftrightarrow} B$$

(证明类似于文献 [4] 中协议 (2) 的证明，只需将 $F_{K_{as}}(\cdots)^S$ 定义为 $\{K_{ab}, N_a\}_{K_{as}}, \{\cdots\}_{K_{ab}},)$．但 B 是不属于 $N-u$ 的，这说明 $-u$ 需要进一步扩展．现增加下列一条规则 (记为 (Ⅳ))．

(Ⅳ) 如果 $P \overset{K}{\longleftrightarrow} Q \wedge P \overset{k}{\text{sees}}_c (K', N-u,)$，则 $x \to P : \cdots, \{\cdots, R, \cdots\}_{K',\cdots} \Rightarrow x \to P : \cdots, \{\cdots, N-(u \cup \{R, Q\}), \cdots\}_{K',\cdots}$．(即若 P 理解 Q 把 N 作为交换密钥 K' 的参照符，则由 K' 加密的主体名也以 N 作为参照符.) 这样，就可避免 $N-u$ 出现上述情况．由这四条规则对协议 (2) 的 A 理想化如下：

$$\left.\begin{array}{l}(1)\ A \to B : A, \{N_a - \{A, S, B\}, A\}_{K_{as}};\\ (2)\ B \to S : A, B, \{N_a - \{A, S, B\}, A\}_{K_{as}}, \{N_b, B\}_{K_{bs}};\\ (3)\ S \to A : \{K_{ab}, N_a - \{A, S, B\}\}_{K_{as'}}, \{B, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}};\\ (4)\ A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}.\end{array}\right\} \tag{3}$$

但若用前三条规则，就不能成功理想化，此例说明增加 (Ⅳ) 是必要的．

如与文献 [4] 中一样，虽然未能证明 (Ⅳ) 的正确性，但它确实有助于对协议的分析．

4 实例分析

本节给出一个实例，BAN 逻辑对此实例的证明是失败的，但若用 $N-u$ 规则进行协议理想化时，则可避免这种证明的失败．这说明 $N-u$ 规则确实有助于协议的分析 (虽未被证明)．

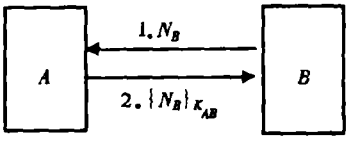

图 2 询问问答协议

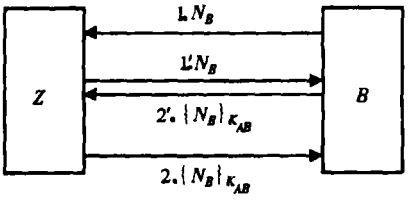

图 3 并行攻击

图 2 的说明：在询问-应答协议中 (图 1)， B 向 A 发出随机数 N_B(询问)，然后， A 向 B 发送 $\{N_B\}_{K_{AB}}$(应答)， K_{AB} 是 A 与 B 的共享密钥；

图 3 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 N_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 N_B， B 收到后，响应发出 $\{N_B\}_{K_{AB}}$, 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 $A|\approx N_B$ (B believes that A has recently said X)。协议的理想化如下：

(1) $B \to A : N_B$,

(2) $A \to B : \{N_B\}_{K_{ab}}$.

初始假设

(1) B believes $fresh(N_B)$,

(2) B believes $\rho(N_B)$(B 相信 N_B 是可以识别的) ,

(3) B received $\{N_B\}_{K_{AB}}$,

(4) B believes $A \overset{K_{AB}}{\longleftrightarrow} B$.

认证目标 B believes A says N_B(B believes that A has recently said N_B)

证明 由 " Necessitation " 规则及初始假设 (2) 和 (3)，我们得到

$$B \text{ belives } B \text{ received}\{N\}_{K_{AB}}.$$

由 " Necessitation " 规则， " Believing " 公理和 " Source Association " 公理和初始假设 (4)，我们得到

$$B \text{ believes } A \text{ said } N_B.$$

把 Necessitation 规则用于 " Freshness " 公理，并注意到初始假设 (1)，我们得到

$$B \text{ believes } A \text{ says } N_B.$$

但图 3 的并行攻击是成功的，即 BAN 逻辑对并行攻击是无能为力的。若用 $N-u$ 规则对此协议进行理想化，则可发现此协议不能够成功理想化。对询问-应答协议 (图 2) 的理想化如下：

(1) $B \to A : N_B - \{\ \}$,

(2) $A \to B : \{N_B - \{\ \}\}_{K_{ab}}$.

我们看到主体 A 不属于集合 u ，说明主体 B 不能了解 A 的 "最近状况"，图 2 的攻击就是利用了协议的这个漏洞， A 没有参加协议的实施，而 B 错误地相信 A 发送了消息 $\{N\}_{K_{AB}}$.

致谢　作者对本文的评审者提出的宝贵意见和建议深表感谢！

参　考　文　献

[1] Butrrows M, Abadi M, Needham R. A logic of authentication, Technical Report SRC Technical Report 39, Digital Equipment Corporation, February 1998.

[2] Abadi M, Tuttle M R. A semantics for a logic of authentication (extended abstract). In Proceedings of Tenth Annual ACM Symposium on Principles of Distributed Computing, At Montreal, Quebec, Canada: August 1991, 201–216.

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

[4] Mao W, Boyd C. Development of authentication protocols: Some misconceptions and a new approach, In Proceedings of Computer Security Foundations Workshop VII. Franconia: IEEE Computer Society Press, 1994, 178–186.

[5] Mao W An augmentation of BAN-like logics. In Proceeding of IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, California: 1995, 44–56.

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

[7] Kesser V, Wedel G. AUOLOG—An advanced logic of authentication. Proc. of the computer Security Foundations Workshop VII, Franconia: IEEE Computer Society Press 1994, 90–99.

A NOTE ON THE AUGMENTATION OF BAN-LIKE LOGICS

Zheng Dong　Tian Jianbo　Wang Yumin

(*Lab.105, Xidian University, Xi'an* 710071)

Abstract　This paper points out a mistake occurred in the Protocol(1)(W.Mao, 1995), the mistake is due to a wrong initial assumption, also this paper shows the weakness of the $N-u$ based-rules. Finaly, an application of the $N-u$ rules is given by an example.

Key words　Authentication protocols, BAN-like logics

郑　东：　男，1964 年生，博士生，从事密码学研究，主要兴趣是密码协议的安全性分析及密码学伪随机性的研究.

田建波：　男，1971 年生，现为复旦大学计算机科学系博士后，从事密码学及网络安全研究，主要兴趣是密码协议的安全性分析及通信网安全协议的设计.

王育民：　男，1936 年生，教授，博士生导师，长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究.