对 BAN 逻辑中新鲜子的研究 [1]

宋荣功 胡正名 杨义先

(北京邮电大学信息安全中心 北京 100876)

摘 要 本文从 BAN 逻辑的基本结构和基本规则出发，对 BAN 逻辑中的新鲜子进行了分析研究，指出 BAN 逻辑在实际应用中不稳固的某些本质原因并不是理想化问题，而是原基本规则中存在的某些问题所致，并进一步对此进行了相应的改进，使得 BAN 逻辑更趋于稳固和完善.

关键词 模态逻辑，BAN 逻辑，新鲜子

中图号 TN918

1 引 言

随着通信技术的迅猛发展，通信的安全问题日益成为人们谈论的热点。近几年来安全协议的设计和分析已受到学术界广泛的关注，引起了人们极大的兴趣，新的科研成果不断涌现，各种新的理论和技术也不断被运用和发展。在安全协议的分析方面，BAN(Burrows M, Abadi M, Needham R) 逻辑 [1,2] 就是其中最著名最重要的一个，其简易性和实用性使其至今为止仍是人们最广泛使用的协议分析工具。但随着人们不断深入地研究，其局限性也逐渐被发现 [3]，为此各种 BAN 逻辑的扩展和改进也不断被提出 [4-6]。

对于 BAN 逻辑的研究，以前主要集中在协议的理想化方面。我们发现虽然人们已花费很多精力对此进行研究，但对某些特殊协议的重放攻击，BAN 逻辑仍然会失效，而且很多理想化的改进又使 BAN 逻辑趋于复杂化，使用起来很不方便，以至于与 BAN 逻辑的简易和实用原则相违背. 近来，我们经过对 BAN 逻辑的基本结构和基本规则进行仔细分析研究发现，之所以 BAN 逻辑在分析这些协议时失败，其本质原因并不全是理想化问题，而是由于 BAN 逻辑中有关新鲜子的规则功能不够或不合理所致，这也是 BAN 逻辑不稳固的一个重要原因。本文一方面对其原因进行了分析，另一方面对其基本规则进行了改进，使其更趋于完善，并且改进后的 BAN 逻辑能有效地对这类协议进行分析，同时又保持了 BAN 逻辑的简易性。

2 BAN 逻辑的缺点

本节我们首先介绍文献 [5] 中的一个密钥分配协议，虽然该协议易受重放攻击，但在文献 [5] 中使用 BAN 逻辑对其进行分析时却很难发现这一缺点. 很多文献 [2,4,5] 认为这是由于 BAN 逻辑的理想化问题所致，并从各自角度提出了各种不同的理想化方法。由于这些理想化方法本身比较复杂且不同的理想化方法其目的也不一致，使得 BAN 逻辑的使用趋于复杂化。实际上，近来经过我们对 BAN 逻辑的基本规则进行研究发现：产生这一问题的本质原因并不是理想化问题，而是某些有关新鲜子的基本规则功能不够或不合理所致。

2.1 一个密钥分配协议 文献 [5] 提出了如下的一个密钥分配协议，该协议要由两个用户 A、B 和一个会话密钥分配机构 S 相互合作才能完成，其中 S 和 A、B 分别有初始的共享密钥 K_{as} 和 K_{bs}, S 的主要作用是为用户 A 和 B 产生新的会话密钥 K_{ab}，并将之传送给用户 A 和 B。该协议成功运行之后的步骤如下：

(1) $A \rightarrow B : A, \{N_a, A\}_{K_{as}}$;

(2) $B \rightarrow S : A, B, \{N_a, A\}_{K_{as}}, \{N_b, B\}_{K_{bs}}$;

(3) $S \rightarrow A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}}$;

[1] 1998-09-17 收到，1998-12-16 定稿
国家自然科学基金重大项目资助，(No.69772035, No.69882002)

(4) $A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$ 。

由文献 [5] 可知当攻击者 C 拥有用户 A 和 B 的一个旧会话密钥 K'_{ab} 时，即 K'_{ab} 已被 C 攻破，该协议就会很容易受到如下的重放攻击：

(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') $C_s \to A : \{K'_{ab}, B\}_{K_{as}}, \{N_a, N_c, \cdots\}_{K'_{ab}}$;

(4) $A \to C_b : \cdots, \{N_c\}_{K'_{ab}}$ 。

并且由文献 [5] 的第二部分可知，使用 BAN 逻辑对其进行分析之后，很容易得到

$$A \text{ believes } A \overset{K'_{ab}}{\longleftrightarrow} B,$$

从而不能有效地发现该重放攻击。

2.2 BAN 逻辑失败分析 为了便于分析，我们把文献 [5] 中的分析步骤总结如图 1 。为了简洁我们使用了文献 [4] 中的符号。

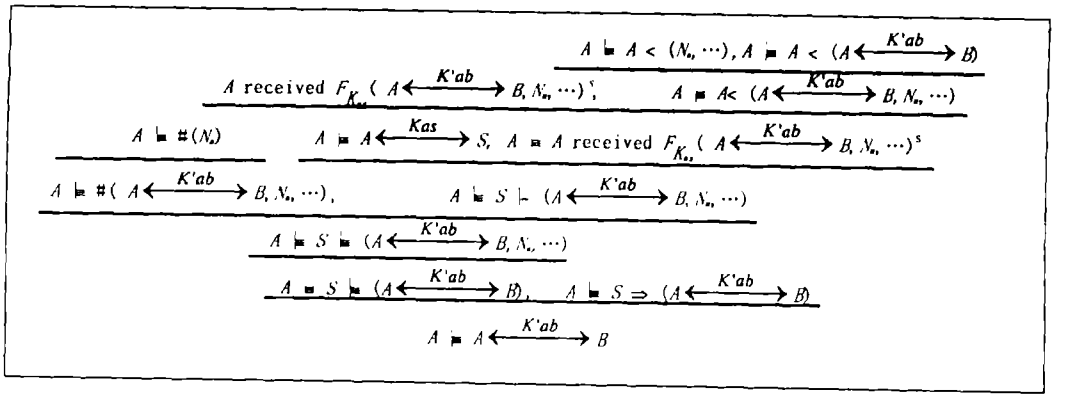

图 1 文献 [5] 中协议的 BAN 逻辑分析过程

由以上 BAN 逻辑分析可知，其实产生失败的原因一方面是由于 BAN 逻辑本身不够完善，而另一方面则是由于错误地运用了 BAN 逻辑本身没有的规则。下面我们分别对其进行分析。

首先，由 BAN 逻辑可知，要想得到 $A \mid\equiv A \overset{K'_{ab}}{\longleftrightarrow} B$，必须要具备条件 $A \mid\equiv S \Rightarrow (A \overset{K'_{ab}}{\longleftrightarrow} B)$ 和 $A \mid\equiv S \mid\equiv (A \overset{K'_{ab}}{\longleftrightarrow} B)$，而想要得到 $A \mid\equiv S \mid\equiv (A \overset{K'_{ab}}{\longleftrightarrow} B)$，就必须具备条件 $A \mid\equiv \#(A \overset{K'_{ab}}{\longleftrightarrow} B)$ 和 $A \mid\equiv S|\sim(A \overset{K'_{ab}}{\longleftrightarrow} B)$ 。虽然 $A \mid\equiv S|\sim(A \overset{K'_{ab}}{\longleftrightarrow} B)$ 可很容易得到，但由于 BAN 逻辑只有从 $A \mid\equiv \#(X)$ 到 $A \mid\equiv \#(X,Y)$ 的规则，而没有从 $A \mid\equiv \#(X)$ 到 $A \mid\equiv \#(Y)$ 的规则，以至于无法得到 $A \mid\equiv \#(A \overset{K'_{ab}}{\longleftrightarrow} B)$，于是便产生上述滥用 BAN 逻辑本身没有而语义又不清楚的规则进行推导的现象，从而使得 BAN 逻辑分析失败。此外我们又不能使用规则：

$$\frac{A \mid\equiv \#(X,Y)}{A \mid\equiv \#(Y)}, \tag{1}$$

因为该规则的语义太模糊，我们将在第 3 节仔细分析其原因。所以我们认为要想 BAN 逻辑避免该类失败，最好是增添从 $A \mid\equiv \#(X)$ 到 $A \mid\equiv \#(Y)$ 的新鲜子规则。

3 BAN 逻辑修改

本节我们首先在 BAN 逻辑的基础上增添两条新的新鲜子规则，然后进一步对新增规则进行语义分析。

3.1 新增新鲜子规则　我们新增的新鲜子规则有两个：一个适合于对称密钥，另一个适合于公开密钥，规则如下：

$$\frac{A \mid\equiv \#(X), A \mid\equiv A \overset{K_{ab}}{\longleftrightarrow} B, A \triangleleft (X,Y)_{K_{ab}}, Y \Leftrightarrow X}{A \mid\equiv \#(Y)}, \tag{2}$$

$$\frac{A \mid\equiv \#(X), A \mid\equiv \overset{K_b}{\longrightarrow} B, A \triangleleft (X,Y)_{K_b^{-1}}, Y \Leftrightarrow X}{A \mid\equiv \#(Y)}, \tag{3}$$

3.2 新增新鲜子规则的语义分析　在分析新增新鲜子规则的语义之前，我们首先分析本文第 2 节中规则 (1) 式不合理的原因。首先我们注意到公式中 (X,Y) 的语义是很模糊的，它没有明确表示 X 和 Y 是否必须要被捆绑在一起，这样它就不能保证 (X,Y) 不会被其他攻击者所改写。事实上 (X,Y) 一旦被攻击者改写，就不可能再得到 $A \mid\equiv \#(Y)$。例如，已知 $A \mid\equiv \#(X)$ 和 $A \triangleleft (X,Y)_{K_{ab}}$，这时只要知道 K_{ab} 的攻击者都可用旧的 Y' 来代替 Y，所以即使推出了 $A \mid\equiv \#(X,Y')$，但也不能保证 $A \mid\equiv \#(Y')$。所以此规则是不合理的，即仅有 $A \mid\equiv \#(X)$ 和 $A \triangleleft (X,Y)$ 是不能得到 $A \mid\equiv \#(Y)$。从以上分析可知在例子中要想得到 $A \mid\equiv \#(Y)$，必须要保证 X 和 Y 是被捆绑在一起的，即保证 $(X,Y)_{K_{ab}}$ 不被其他人改写，这样就必须要具备条件 $A \mid\equiv A \overset{K_{ab}}{\longleftrightarrow} B$，这也正是新增规则 (2) 式的条件之一。下面我们来具体分析一下规则 (2) 和 (3) 式。

我们知道要从已知条件 $A \mid\equiv \#(X)$ 和 $A \triangleleft (X,Y)$ 得到 $A \mid\equiv \#(Y)$，必须保证 X 和 Y 被捆绑在一起，即保证 (X,Y) 不会被其他人改写或重放，这就要求 (X,Y) 要被加密或签名，并且 A 要相信该加密钥或公开钥，亦即要具备条件 $A \triangleleft (X,Y)_{K_{ab}}$ 和 $A \mid\equiv A \overset{K_{ab}}{\longleftrightarrow} B$ 或 $A \triangleleft (X,Y)_{K_b^{-1}}$ 和 $A \mid\equiv \overset{K_b}{\longrightarrow} B$。除此之外，还要求 Y 是一次性消息，即要求 Y 同 X 一样是随着协议的不同建立而变化，并且只与协议的该次建立紧密相关，为方便我们用 $Y \Leftrightarrow X$ 表示 Y 的上述性质。反之具备了条件 $A \triangleleft (X,Y)_{K_{ab}}$ 和 $A \mid\equiv A \overset{K_{ab}}{\longleftrightarrow} B$ 或 $A < (X,Y)_{K_b^{-1}}$ 和 $A \mid\equiv \overset{K_b}{\longrightarrow} B$，就保证了 A 相信 (X,Y) 不会被其它攻击者改写或重放，即保证了 X 和 Y 是捆绑在一起的，这样再加上条件 $A \mid\equiv \#(X)$ 和 $Y \Leftrightarrow X$，就可保证 $A \mid\equiv \#(Y)$ 了。从以上分析可知新增的规则是完全正确的，其语义是合理的。

4 新逻辑规则的应用

现在我们使用新的 BAN 逻辑规则再来分析一下 2.1 节中的例子，首先由于 BAN 逻辑本身并没有以下规则：

$$\frac{A \mid\equiv A \overset{K_{as}}{\longleftrightarrow} S, A \mid\equiv A \triangleleft F_{K_{as}}(A \overset{K'_{ab}}{\longleftrightarrow} B, N_a, \cdots)^S}{A \mid\equiv S \mid\sim (A \overset{K'_{ab}}{\longleftrightarrow} B, N_a, \cdots)},$$

而且这条规则的语义也极不合理，所以我们不能再使用这条规则，只能使用 BAN 逻辑本身相应的规则：

$$\frac{A \mid\equiv A \overset{K_{as}}{\longleftrightarrow} S, A \triangleleft (A \overset{K'_{ab}}{\longleftrightarrow} B)_{K_{as}}}{A \cdot \mid\equiv S \mid\sim (A \overset{K'_{ab}}{\longleftrightarrow} B)}.$$

这样要想得到 $A \mid\equiv A \overset{K'_{ab}}{\longleftrightarrow} B$，就必须首先推出 $A \mid\equiv \#(A \overset{K'_{ab}}{\longleftrightarrow} B)$。由新规则 (2) 式可知，这就必须具备条件 $A \mid\equiv \#(X)$, $A \mid\equiv A \overset{K_{as}}{\longleftrightarrow} S$, $A \triangleleft (X, A \overset{K'_{ab}}{\longleftrightarrow} B)_{K_{as}}$, $K'_{ab} \Leftrightarrow X$。显然原协议不具备该条件，从而也无法推出 $A \mid\equiv A \overset{K'_{ab}}{\longleftrightarrow} B$。而改进后的 BAN 逻辑能有效地对该协议进行分析；并且进一步由新增规则可知，对该协议修改的最好方法是在第 (3) 步把 N_a 放在 $(A \overset{K_{ab}}{\longleftrightarrow} B)_{K_{as}}$ 中，使 N_z 和 K_{ab} 捆绑在一起，即第 (3) 步应改为

(3) $S \rightarrow A : \{N_a, K_{ab}, B\}_{K_{as}}, \{N_a, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}}$。

5 小 结

本文对 BAN 逻辑的新鲜子进行了仔细分析，提出了能满足捆绑机制的新的新鲜子规则，并进一步分析了其语义的合理性，通过应用证明了改进后的 BAN 逻辑确实比以前更加完善。

参 考 文 献

[1] Burrows M, Abadi M, Needham R. A logic of authentication. Technical Report SRC Technical Report 39, Digital Equipment Corporation, February, 1989.

[2] Abadi M, Tuttle M R. A semantics for a logic of authentication. In Proceedings of Tenth Annual ACM Symposium on Principles of Distributed Computer Science, New York: 1991, 201–216.

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

[4] Mao W, Boyd C. Towards formal analysis of security protocols. In Proceedings of Computer Security Foundations Workshop VI, Washington: IEEE Computer Society Press, 1993, 147–158.

[5] Mao W. An augmentation of BAN-like logics. In Proceedings of Computer Security Foundations Workshop VIII, Washington: IEEE Computer Society Press, 1995, 44–56.

[6] van Oorschot P C. An alternate explanation of two BAN-logic "failures". In Lecture Notes in Computer Science 765, Berlin: Springer-Verlag, 1993, 443–447.

THE INVESTIGATION OF THE FRESHNESS IN BAN LOGIC

Song Ronggong Hu Zhengming Yang Yixian

(*Dept. of Infor. Eng., Beijing University of Posts and Telecommunications, Beijing* 100876)

Abstract Based on BAN's basic constructs and rules, the freshness in BAN logic is investigated. In this paper it is presented that some reasons why BAN logic is in practice unsound are not idealization problems, but problems what some basic rules result in. For the latter, a modified method is proposed to avoid similar problems.

Key words Modal logic, BAN logic, Freshness

宋荣功： 男，1967 年生，博士生，主要研究方向为：信息安全，安全协议分析，密钥管理.

胡正名： 男，1931 年生，教授，主要研究方向为：编码学，密码学.

杨义先： 男，1961 年生，教授，主要研究方向为：编码学，密码学，信息安全，网络安全.