“对 BAN 逻辑中新鲜子的研究”的注记 [1]

袁 丁 *** 范平志 * 何明星 *

*(西南交通大学移动通信研究所 成都 610031)
**(四川大学电子信息学院 成都 610064)

摘 要 该文通过一个反例说明，宋荣功等“对 BAN 逻辑中新鲜子的研究”中关于 BAN 逻辑新鲜子规则条件过于严格，可能把一个安全的协议分析成不安全的协议.

关键词 密码协议，BAN 逻辑，新鲜子
中图号 TN918.1

1 引 言

90 年代以来，密码协议的形式化成为国际上研究的热点. 这种方法的出发点是希望将密码协议形式化，再借助于人工推导和计算机的辅助分析，来判断密码协议是否安全可靠. 其中，BAN(Burrows M， Abadi M， Needham R) 逻辑 [1] 是最早提出，也是最为重要的一种安全协议分析方法. 利用该逻辑已成功地发现了许多著名协议存在的漏洞. 但是，它本身的局限性也逐渐被发现 [2−8] . 第一， BAN 逻辑只能分析密码协议的某一子集；第二， BAN 逻辑有时会把一个有安全缺陷的密码协议证明是安全的.

文献 [4-6] 认为 BAN 逻辑在分析某些协议之所以失败，是由于理想化过程出现了故障. 文献 [7] 对 BAN 逻辑语义的精确化进行了改进. 文献 [8] 认为， BAN 逻辑在分析某些协议之所以失败的重要原因不全是理想化问题，而是 BAN 逻辑中有关新鲜子的规则功能不够或不合理所致，并对 BAN 逻辑的有关新鲜子的规则进行了扩展.

本文认为 BAN 逻辑确实存在缺陷. 但是，文献 [8] 扩展的新鲜子规则条件太强，有不尽合理的地方：可能把安全的协议分析成不安全的协议. 下面首先介绍文献 [8] 的基本思想，并用一个反例说明文献 [8] 扩展的新鲜子规则不尽合理.

2 文献 [8] 的基本思想

下面的一个密钥分配协议有两个通信主体 A， B 和一个密钥分配机构 S 相互作用完成密钥分配. 其中， K_{as}， K_{bs} 分别是 S 和 A 以及 S 和 B 的共享密钥， S 的作用是为 A 和 B 产生会话密钥 K_{ab}， N_a 和 N_b 分别由 A 和 B 产生的大随机数 (新鲜子) . 该协议的运行步骤如下 [8] ：

$$\text{M1 } A \to B : A, \{N_a, A\}_{K_{as}}$$
$$\text{M2 } B \to S : A, B, \{N_a, A\}_{K_{as}}, \{N_b, B\}_{K_{bs}}$$
$$\text{M3 } S \to A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_b, \{K_{as}, A, N_b\}_{K_{bs}}\}_{K_{ab}}$$
$$\text{M4 } A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$$

由 BAN 逻辑很容易得到：

[1] 2001-02-26 收到， 2001-10-15 定稿
国家自然科学基金资助课题 (NSFC 资助号： 69825102)

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

但是，这个由 BAN 逻辑分析证明正确的协议，不能抵抗重传攻击．设攻击者 C 存储一条旧报文 $\{K_{ab}, B\}_{k_{as}}$，并从中破译出旧的会话密钥 K_{ab}，则 C 可以做如下攻击：

M1 $A \to C : A, \{N_a, A\}_{K_{as}}$， C 截获 A 发给 B 的报文 M1．

M2 $C \to S : C, A, \{N_c, C\}_{K_{cs}}, \{N_a, A\}_{K_{as}}$， C 冒充 B 把报文 M2 发给 S．

M3 $S \to C : \{K_{ca}, A\}_{K_{cs}}, \{N_c, N_a, \{K_{ca}, C, N_a\}_{K_{as}}\}_{K_{ca}}$， S 误认为是 $C - A - S$ 间的正常通信，故把报文 M3 发给 C．

M3′ $C \to A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_c, \#\#\#\}_{K_{ab}}$， C 冒充 S 把报文 M3′ 发给 A，其中 $\#\#\#$ 可为任意值．

M4 $A \to C : \{\#\#\#\}_{K_{bs}}, \{N_c\}_{K_{ab}}$， C 冒充 B 截获报文 M4．

这样，C 成功地使 A 相信，A 和 B(C) 之间获得一轮新的会话密钥 K_{ab}．以后，C 就可以冒充 B，利用 K_{ab} 进一步获取 A 的机密。

显然，上述协议并不完全安全，但利用 BAN 逻辑可以证明它是安全的．文献 [8] 认为，BAN 逻辑在分析某些协议之所以失败，很大原因在于 BAN 逻辑中有关新鲜子的规则功能不够或不合理所致，并扩展了两个新鲜子的规则：一个适合于对称密钥，另一个适合于公开密钥．其规则如下：

$$\frac{A| \equiv \#(X), A| \equiv A \overset{K_{ab}}{\longleftrightarrow} B, A \triangleleft (X, Y)_{K_{ab}}, y \Longleftrightarrow X}{A| \equiv \#(Y)} \tag{1}$$

$$\frac{A| \equiv \#(X), A| \equiv A \overset{K_b}{\mapsto} B, A \triangleleft (X, Y)^{-1}_{K_b}, y \Longleftrightarrow X}{A| \equiv \#(Y)} \tag{2}$$

最后，文献 [8] 的作者用规则 (1) 式证明该协议并不安全．实际上，只有当会话密钥与新鲜子捆绑发送时，用文献 [8] 的新鲜子规则才可以得到协议是安全的结论．

3 一个反例

我们只需将上述协议稍加修改：即将 B 发给 S 的报文 $\{N_b, B\}_{K_{bs}}$ 改为 $\{N_b, A\}_{K_{bs}}$， A 经 B 发给 S 的报文 $\{N_a, A\}_{K_{as}}$ 改为 $\{N_a, B\}_{K_{as}}$，上述协议就变得安全了．具体的协议如下：

M1 $A \to B : A, \{N_a, B\}_{K_{as}}$

M2 $B \to S : A, B, \{N_a, B\}_{K_{as}}, \{N_b, A\}_{K_{bs}}$

M3 $S \to A : \{K_{ab}, B\}_{K_{as}}, \{N_a, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{ab}}$

M4 $A \to B : \{K_{ab}, A, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$

假设用上面的攻击方法对该协议实施重传攻击．攻击者 C 截获 A 发给 B 的报文 $A, \{N_a, B\}_{K_{as}}$，C 接着冒充 B 把报文 $C, A, \{N_c, A\}_{K_{cs}}$， $\{N_a, B\}_{K_{as}}$ 发给 S，由于 S 可以判断出通信实体之间的身份并不一致，故 S 将终止协议的运行，从而防止了上面的重传攻击．该协议之所以是安全的，主要是因为协议建立了 N_a 与 B， N_b 与 A 之间的完整性联系 [6]．但是，用文献 [8] 的新鲜子规则却无法证明该协议是安全的．证明如下：由于有 $A| \equiv A \overset{K_{as}}{\longleftrightarrow} S$， $A \triangleleft (A \overset{K_{ab}}{\longleftrightarrow} B)_{K_{as}}$，

则 $A| \equiv S| \sim (A \overset{K_{ab}}{\longleftrightarrow} B)$．这样要想得到 $A| \equiv A \overset{K_{ab}}{\longleftrightarrow} B$，就必须首先得到 $A| \equiv \#A \overset{K_{ab}}{\longleftrightarrow} B)$．由新规则 (1) 式可知，就必须具备条件 $A| \equiv \#(X)$，$A| \equiv A \overset{K_{as}}{\longleftrightarrow} S$，$A \triangleleft (X, A \overset{K_{ab}}{\longleftrightarrow} B)_{K_{as}}$，$K_{ab} \Longleftrightarrow X$．显然，该协议不具备此条件，从而也无法推出 $A| \equiv A \overset{K_{ab}}{\longleftrightarrow} B$，即无法证明该协议是安全的．

4 结　论

BAN 逻辑作为目前最有影响的一种形式化分析工具，在协议的安全性分析方面得到了广泛的应用．但是，它还存在很多不完善的地方．文献 [8] 在这方面进行了积极的探索．但文献 [8] 扩展的关于新鲜子的规则条件过于严格，存在不尽合理的地方，有待进一步改进．

参　考　文　献

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

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

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

[4] L. Gong, R. Needham, R. Yahalom, Reasoning about belief in cryptographic protocol, Proc. , IEEE Symp. Security and Privacy, Oakland, Calif., 1990, 234–248.

[5] B. Syverson, Paul, V. Oorschot, On unifying some cryptographic protocol logics, Proc. IEEE Symp., Security and Privacy, Oakland, Calif., 1994, 14–28.

[6] 卿斯汉，关于密码协议分析的注记，China Crypt'96, Zhengzhou, 1996, 214–219.

[7] 郑东，王常杰，王育民，一种 BAN 逻辑的修正，电子科学学刊，2000, 22(4), 579–584.

[8] 宋荣功，胡正名，杨义先，对 BAN 逻辑中新鲜子的研究，电子科学学刊，2000, 22(3), 505–508.

NOTES ON THE INVESTIGATION OF THE FRESHNESS IN BAN LOGIC

Yuan Ding* **　　Fan Pingzhi*　　He Mingxing*

*(*Institute of Mobile Comm., Southwest Jiaotong University, Chengdu* 610031, *China*)

**(*School of Electronic Information, Sichuan University, Chengdu* 610064, *China*)

Abstract　In this paper, it is pointed out by a counterexample that the condition of the freshness rule on BAN logic which in the paper "The Investigation of the Freshness in BAN Logic" written by Song Ronggong, *et al.* is so strict that it regards possibly a secure protocol as an insecure protocol.

Key words　Cryptographic protocol, BAN logic, Freshness

袁　丁：　男，1967 年生，讲师，研究方向：信息安全，电子商务．

范平志：　男，1955 年生，教授，研究方向：信息安全，移动通信．

何明星：　男，1964 年生，副教授，研究方向：信息安全，电子商务．