云南大学学报 (自然科学版), 2005, 27 (1): 18~ 21 CN 53- 1045/N ISSN 0258- 7971
Journal of Yunnan University

# 多播水印协议 MAMWP 的 BAN 逻辑分析*

陆正福, 叶 锐, 王国栋
(云南大学 数学系, 云南 昆明 650091)

摘要: 用形式化的方法分析密码协议可以检测出协议中的漏洞和证明协议的安全性, BAN 类逻辑是目前使用最广泛的一种形式化分析密码协议的方法. 文章介绍了基于移动代理的多播水印协议 MAMWP 和 BAN 逻辑, 并给出了用 BAN 逻辑分析 MAMWP 协议的详细过程.

关键词: 多播水印协议; BAN 类逻辑; 移动代理; 数字水印; 数字指纹
中图分类号: TP 393.08 文献标识码: A 文章编号: 0258- 7971(2005)01- 0018- 04

一般将利用数字水印和数字指纹在多播环境中实现版权认证、盗版源跟踪、泄密者识别等功能的协议称为多播水印协议(下文简称 MWP). 对单播和多播, 我们都可在数据中嵌入稳健数字水印以证实数据的版权所有者. 对于数字指纹则不然, 在多播方式下, 如果在多播数据之前把指纹嵌入到数据中, 由于每个组成员接收到的数据都相同, 包含在数据中的指纹也相同, 这与指纹要求的唯一性相背离. 多播与指纹要做到 2 种技术共存, 就必须重新设计有关的 MWP 协议, 以求得性能和安全的综合平衡, 此即 MWP 研究面临的主要问题. 在文献[1]中我们提出了一个基于移动代理(MA)的多播水印协议 MAMWP, 形成解决多播和指纹矛盾的一个新协议. MAMWP 综合了 WHIM 协议[2]和 SMPCP 协议[3]的优点, 避免了 WHIM 协议过分依赖中间实体安全性和计算能力的缺点, 也避免了 SMPCP 协议的一些性能缺陷. MAMWP 协议的特点在于: ①它不依赖于中间节点的安全性及计算能力, 可以实现于任何一个已经存在的多播体系结构之上; ②它第一次把组密钥引入到 MWP 协议的设计中, 利用了多播本身的特点, 而且使协议可以利用多播组密钥管理的研究成果; ③它可以支持动态的组成员身份, 具有可扩展性. 这只需要在组成员变动时更新组密钥即可; ④协议可在异构环境中运行, 可在跨平台环境中工作; ⑤由 MA 实现每个用户接收到的数据流的唯一性; ⑥协议牺牲带宽以实现指纹的唯一性.

文献[1]关注的是 MAMWP 协议的设计以及与其它同类协议的比较, 本文关注的则是协议安全性的形式化分析.

本文采用如下记号约定: S 表示多播组中的数据发送者, S_ID 是 S 的标识, S_key, S_key′ 分别表示 S 的私钥和公钥. $U_i$ 表示第 $i$ 个多播组成员, $U_i$_ID 是 $U_i$ 的标识, $U_i$_key, $U_i$_key′ 分别表示 $U_i$ 的私钥和公钥. CA 表示认证中心, CA_key, CA_key′ 分别表示 CA 的私钥和公钥. $d_1, d_2, \cdots, d_n$ 表示待发数据, $d_j^{w_0}$, $d_j^{w_1}$ 表示嵌入水印 $w_0$ 和 $w_1$ 后的数据. C_$U_i$ 表示用户 $U_i$ 的数字证书. $\{M\}_K$ 表示用密钥 $K$ 加密消息 M, SessionID 是会话标识.

## 1 MAMWP 中有待分析的协议环节

MAMWP 协议安全性主要包括如下的内涵: 首先是指协议对数据的版权保护能力, 这是 MWP 设计和分析的重点, 对于 MAMWP 还应考虑 MA 的安全性. 这些是文献[1]讨论的重点. 其次是作为一般安全协议含义上的安全性, 因为该协议的数据传输前的准备阶段包含了认证、密钥交换等一般安全协议的环节, 需加以形式化的描述和分析; 安全协议的形式化分析技术目前主要有 3 类, 分别是基

* 收稿日期: 2004- 03- 17
基金项目: 云南省自然科学基金资助项目(2002F0012M); 云南大学理(工)科校级科研项目资助(2003Z010C).
作者简介: 陆正福(1965- ), 男, 安徽人, 副教授, 主要从事协议工程、信息安全和网络计算方面的研究.

于推理的(以 BAN 逻辑为代表)、基于攻击的和基于证明的三类结构性方法. 本文所做的研究工作是采用 BAN 逻辑来推证 MAMWP 数据传输前的准备阶段是安全的.

下面介绍 MAMWP 协议数据传输前的准备阶段.

协议需满足的前提条件有: ①CA 和 S 的公钥是公开的; ②当用户申请加入一个多播组时, 即表明该用户信任这个多播组的发送者 S 和他发送的 MA; ③S 已经在 CA 处注册了 2 个水印 $w_0$ 和 $w_1$.

数据传输前的准备阶段具体如下:

(1) 用户 $U_i$ 申请加入一次多播会话, 发送加入请求和数字证书给 S:

$\{\text{join request, SessionID, } U_i\_\text{ID, C\_}U_i, U_i\_\text{key}'\}_{S\_key'}$.

(2) S 用自己的私钥解密之, 并将 $C\_U_i$ 提交 CA, 请求验证用户 $U_i$ 的合法性:

$\{S\_\text{ID}, U_i\_\text{ID}, C\_U_i\}_{CA\_key'}\}$.

(3) CA 将验证结果告知 S:

$\{\{\text{Valid/ InValid}, U_i\_\text{ID}\}_{CA\_key}\}_{S\_key'}$.

(4) 若 $C\_U_i$ 没有通过验证, 则 S 发送一个拒绝加入消息到 $U_i$, 并结束和 $U_i$ 的通话:

$\{\{\text{Rejection, SessionID}\}_{S\_key}\}_{U_i\_key'}$.

若 $C\_U_i$ 通过验证, 则 S 为 $U_i$ 生成一个 MA, MA 中包含用户 $U_i$ 的指纹 $f_{Ui}$和必要的信息, 并使 MA 移动到 $U_i$:

$\{\{\text{MA, SessionID}\}_{S\_key}\}_{U_i\_key'}$.

(5) 用户 $U_i$ 鉴别 MA 是否是 S 发送的. 若是, 则允许 MA 在本地主机上执行, 并发送 MA 到达的确认 ACK 给 S; 否则, 不允许 MA 执行.

确认 ACK:

$\{\{\text{Confirmation, SessionID}\}_{U_i\_key}\}_{S\_key'}$.

限于篇幅, MAMWP 协议的完整描述可参考文献[1].

## 2　基于 BAN 逻辑的协议安全性分析

**2.1　BAN 逻辑的表达式和推理规则**　BAN 逻辑[4]是一个关于信念的形式逻辑模型, 它有规定的逻辑符号和推理公式, 它的出现开创了用形式逻辑证明协议安全性的先例, 引发了一批后继的研究. 尽管后来发现它具有某些不足, 但是与后继的逻辑系统相比, 它以简明性获得了广泛的应用. 而针对它的不足之处, 关键在于要注意协议的初始假设和理想抽象的语义正确性, 这样才能保证逻辑推理结果的正确性.

下面给出本文所使用的 BAN 逻辑表达式和推理规则.

(1) 表达式:

P believes X 表示 P 相信 X 是真实的;

P sees X 表示 P 看见 X, 如 P 收到含有 X 的消息;

P said X 表示 P 曾经说过 X, X 可能是现在发送的, 也可能是以前发送的;

P controls X 表示 P 对 X 有控制权, 如 P 能生成随机性很好的密钥;

# (X) 表示 X 是新鲜的, 即没有用过的;

SK(P, Q; K) 表示 K 是 P 和 Q 之间通信密钥;

PK(P; K) 表示 K 是 P 的公钥;

SV(P, Q; X) 表示 X 是 P 和 Q 之间的秘密值;

$\{X\}_K$表示 X 用 K 加密.

(2) 推理规则:

消息意义规则(Message- meaning Rule):

$$①\ \frac{\text{P believes SK(P, Q; K), P sees } \{X\}_K}{\text{P believes Q said X}},$$

表示为 P 相信 K 是 P 和 Q 之间的通信密钥, 当 P 看到用 K 加密的信息 X, 则 P 相信 Q 曾经说过 X.

$$②\ \frac{\text{P believes PK(Q; K), P sees } \{X\}_K^{-1}}{\text{P believes Q said X}},$$

与上同理.

随机数验证规则(None- verification Rule):

$$③\ \frac{\text{P believes \# (X), P believes Q said X}}{\text{P believes Q believes X}},$$

表示 P 相信 X 是新鲜的, 且 P 相信 Q 曾经说过 X, 则 P 相信 Q 相信 X 是真实的.

裁判规则(Jurisdiction Rule):

$$④\ \frac{\text{P believes Q controls X, P believes Q believes X}}{\text{P believes X}},$$

表示 P 相信 Q 对 X 有控制权, 且 P 相信 Q 相信 X, 则 P 也相信 X.

$$⑤\ \frac{\text{P believes \# (X)}}{\text{P believes \# (X, Y)}},$$

如果 P 相信消息部分是新鲜的, 则整个消息是新鲜的.

⑥ $\frac{\text{P believes PK(P; K), P sees } \{X\}_K}{\text{P sees X}}$,

如果 P 看到用自己有效公钥加密的信息,则 P 可以解密看到的信息.

**2.2** 初始信任与推证结果 BAN 逻辑是基于知识和信任,使用推理规则来分析的.

在分析协议前,先要假设一组初始信任,随着协议的运行,每接收到一条消息都映射到信任集,结合初始信任(初始信任在协议运行时是不变的),用推理公式推出新的信任,到最后信任集满足所要达到的目标,则认为协议是正确的. 如信任集不能满足,则可引导发现协议的缺陷.

不同的密码协议,需要推证不同的结果. 对于安全认证类协议,身份认证是在保密通信之前,因此希望在保密通信之前,信任要达到某种状态. 比如说,A 与 B 之间要建立会话密钥 K,那么在用会话密钥 K 通信之前,信任达到以下目标,我们认为认证是完整的.

即: A believes SK(A, B; K) A 相信 K 是 A, B 之间通信的好密钥;

B believes SK(A, B; K) B 相信 K 是 A, B 之间通信的好密钥.

有的密码协议还可以得到进一步的结论:

A believes B believes SK(A, B; K) A 相信 B 相信 K 是 A, B 之间通信的好密钥;

B believes A believes SK(A, B; K) B 相信 A 相信 K 是 A, B 之间通信的好密钥.

在下文可见,MAMWP 协议的推证结果属于上述 2 种类型.

**2.3** **MAMWP** 协议模型化 只考虑用户 U 是合法用户的情况,得到如下流程:

消息(4): $S \rightarrow U: \{\{SV(S, U; X_{SU}), N\}_{K_S^{-1}}\}_{K_U}$;

消息(5): $U \rightarrow S: \{\{SV(S, U; X_{SU}), N\}_{K_U^{-1}}\}_{K_S}$.

由于只考虑合法用户的情况,即消息(1),(2),(3)可以忽略,因此不对它们进行理想化.

消息(4)中由于 MA 包含着交换的共享密钥,因此直接用逻辑符号 $SV(S, U; X_{SU})$ 表示 S 和 U 之间的共享密钥,会话标识 SessionID 也与安全有关,因此将它理想化出来.

消息(5)同理.

注意协议的模型化涉及对 MA 结构的理解. 事实上,MAMWP 协议中的 MA 包含专门的程序和与安全有关的数据. MA 可采用固定的结构,包括如下功能模块: 通信接口模块: 将内部机制与外界分离,与其执行环境及数据发送者交换数据. 安全控制模块: 提供 MA 自身的保护,执行 MA 的安全策略,阻止外界环境对 MA 的非法访问. 代码模块: 包括 MA 要执行的代码对象. 约束条件: 是数据发送者为保证 MA 的行为和性能而作出的约束,如执行时间极值、站点停留时间及任务完成程度等. 信息模块: 包括 MA 的密钥(专用密钥和组密钥)、用户的指纹. 内部状态集: 是 MA 执行过程中的当前状态,它影响 MA 的代码执行过程.

**2.4** 协议分析 我们先给出假设:

①S believes $PK(U; K_U)$;

②U believes $PK(S; K_S)$;

③S believes $SV(S, U; X_{SU})$;

④U believes S controls $SV(S, U; X_{SU})$;

⑤S believes # (N);

⑥U believes # (N).

前 2 个假设 S 相信 $K_U$ 是 U 的公钥,U 相信 $K_S$ 是 S 的公钥,因为协议的前提条件假设 S 的公钥是已知的,并假设 U 是合法用户,所以这 2 个假设是可行的. ③是 S 相信 $X_{SU}$ 是 S 和 U 之间的共享密钥, ④是 U 相信 S 能够生成 U 和 S 之间的共享密钥 $X_{SU}$. 由于 $X_{SU}$ 是由 S 生成的,因此这 2 个假设是可行的. 最后 2 个假设,S 相信 N 是新鲜的,U 相信 N 是新鲜的.

协议分析过程如下:

由假设①和消息(4),根据规则(6)得:

U sees $\{SV(S, U; X_{SU}), N\}_{K_S^{-1}}$,

且 U believes $PK(S; K_S)$,根据规则(2)得

U believes S said $(SV(S, U; X_{SU}), N)$,

再根据假设⑥和规则(5),(3)得

U believes S believes $SV(S, U; X_{SU})$ (a),

由假设④和(a),根据规则(4)得

U believes $SV(S, U; X_{SU})$ (b),

由假设②和消息(4),根据规则(6)得

S sees $\{SV(S, U; X_{SU}), N\}_{K_U^{-1}}$,

且 S believes $PK(U; K_U)$,根据规则(2)得

S believes U said $(SV(S, U; X_{SU}), N)$,

再由假设⑤和规则(5),(3)得

S believes U believes $SV(S, U; X_{SU})$ (c),

因此,总的结果为(a),(b),(c)和③,即

S believes $SV(S, U; X_{SU})$,

U believes SV(S, U; $X_{SU}$),

S believes U believes SV(S, U; $X_{SU}$),

U believes S believes SV(S, U; $X_{SU}$),

最终的信任集表明, MAMWP 数据传输前准备阶段的认证工作是完整的、没有漏洞的, 实现了通信各方共享密钥的目标.

## 3 结　论

本文用BAN 逻辑以演绎推理的方式分析了我们在文献[1] 中设计的多播水印协议, 证明了 MAMWP 协议数据传输前准备阶段的安全性, 即证明了协议双方的认证是完整的、没有漏洞的. 就整个协议的安全性而言, 还涉及移动代理的安全性、盗版者跟踪与泄漏者识别等, 这些问题在文献[1]中已有所讨论. 本文的分析工作是对 MAMWP 协议研究的深化和完善.

应该指出的是, 从理性上讲, 演绎式的逻辑推证是最能令人信服的证明手段之一. 然而初始信任假设、协议模型化(又称理想化) 不是形式化的演绎, 而它又是BAN 逻辑分析的关键步骤之一, 因此不适当的理想化与不正确的初始信任, 会导致分析结果出现逻辑分析的典型困难: 被证明安全的协议一定安全吗? 因此作为协议的设计者、分析者以及使用者都应该正确地遵循初始信任集、恰当地进行理想化.

## 参考文献:

[1] 陆正福, 叶　锐, 王国栋. 基于移动代理的多播水印协议[J]. 云南大学学报(自然科学版), 2004, 26(4): 306－311.

[2] JUDGE P, AMMAR M. WHIM: Watermarking multicast video with a hierarchy of intermediaries[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2002, 39(6): 699－712.

[3] CHU Hao-hua, QIAO Lin-tian, NAHRSTEDT K. A secure multicast protocol with copyright protection[A]. Proceedings of the IS&T/SPIE Conference on Security and Technology[C]. Calif San Jose, 1999. 460－471.

[4] BURROW M, ABADI M, NNNEHAM R. A logic of authentication[J]. ACM Transaction in Compute System, 1990, 2: 18－36.

# BAN logic analysis of MAMWP protocol

LU Zheng-fu, YE Rui, WANG Guo-dong

(Department of Mathematics, Yunnan University, Kunming 650091, China)

**Abstract**: Formal methods can be useful to detect errors and prove security in cryptographic protocols. BAN-like logic has been the most widely used formal method by far. It is discussed the MAMWP protocol and BAN logic, and discribled a process of analysis of MAMWP protocol using BAN logic.

**Key words**: multicast watermarking protocol; BAN-like logic; mobile agent; watermarking; fingerprinting