A New Logic for the Design of Authentication Protocol

ZHENG Jun-jie[1] YE Song[1] LIU Zhi-hua[1] MA Ying[2] MA Jin-gang[1]

1.Institute of meteorology, Liberation Army University of Science and Technology, Nanjing, China

2. Training department, Liberation Army University of Science and Technology, Nanjing, China

Email：1. e-mail :oldwolf0411@sina.com,

Abstract: It was a very difficult task for researchers to design the security protocol which satisfy the security goal. Nowadays the researchers are absorbed in the analysis and verification for security protocol's safety property by using formal methods. A new logic using for the design of authentication protocol based on BAN and GNY logic was presented. The channel mechanism in PI calculus was introduced and the distributed system was described by this mechanism. The safety goal of Woo-Lam protocol was analyzed and the protocol was designed again by the new logic, the result shows that the logic was helpful to the design of security protocols.

Keywords: security protocol; logic; design; Woo-Lam protocol

一种设计认证协议的简单逻辑

郑君杰[1] 叶松[1] 刘志华[1] 马英[2] 马金钢[1]

1. 解放军理工大学气象学院，南京, 中国；2. 解放军理工大学训练部，南京, 中国

Email：1. e-mail :oldwolf0411@sina.com

【摘要】设计出符合安全目标的安全协议是十分复杂与困难的过程，目前研究者更多地专注于使用形式化方法对现有的安全协议进行分析与验证。在 BAN 与 GNY 逻辑的基础上提出一种新的逻辑可用于认证协议的设计，介绍了新逻辑的语法、推导规则与分解规则等，同时引入 Pi 积分中的信道机制对分布式系统进行刻画。重新分析了 Woo-Lam 认证协议的安全性目标，使用提出的逻辑与信道机制重新进行协议的设计，结果证明是有效的。

【关键词】安全协议；逻辑；设计；Woo-Lam 协议

1. 引言

安全协议（security protocol）又叫做密码协议（cryptographic protocol），是使用了密码学方法的网络通信协议，其目的就是为了在复杂的、不安全的网络分布式系统环境中提供各种安全服务，人们通过安全协议来具体实现安全共享网络资源的需求[1]。

目前研究者更多地专注于使用形式化方法对现有的安全协议进行分析与验证[2-3]，但是如果从安全协议的设计阶段就开始应用形式化的方法，设计出的协议将更加安全、有效。本文在 BAN 与 GNY 逻辑的基础上提出了一种新的抽象逻辑作为认证协议的设计工具，可以在高的抽象级别对认证协议进行逻辑抽象，提出了分解规则用于协议的设计，引入 Pi 积分[4]中信道的概念，使用信道进行不同的访问控制，不必考虑协议的具体执行。首先，协议设计者需要明确协议的目标,然后使用本逻辑对协议的目标进行刻画，通过使用分解规则，看分解后的目标是否满足，最后产生整个协议。这种方法得到的结果是直观的形式化的描述。

国家自然科学基金(40976062)
江苏省自然科学基金(BK2009062)
解放军理工大学气象学院基础理论基金
解放军理工大学气象学院博士启动基金
解放军理工大学预先研究基金

2. 基于 PI 积分的信道模型

Pi 积分是一个小型的但是有很强表达力的程序语言，Pi 积分程序系统包括独立的、并行的、通过在信道上进行消息握手而同步的进程，信道可以是受限的，因此只有某些程序可以在信道上通信。

把分布式系统视为参与者（包括用户、主机和进程等等）与信道的集合，信道是有访问属性的通信设

978-1-935068-23-5

施的抽象，可以表达一个物理链接，或者是参与者之间的安全逻辑连接，因此可用信道模拟安全服务，代替以往逻辑中使用的加密、解密等操作。参与者之间可以根据预先定义的规则进行交互，而这种交互是通过基于信道所进行的消息的传送来实现的。一个信道可以通过它的接收者与发送者的集合来进行刻画。将信道定义为 C，则接收者的集合和发送者的集合分别可以表示为 $r(C)$ 和 $w(C)$。假设 P、Q 是参与协议的两个主体，它们之间可以经由信道 C 安全地交换信息，则 $r(C) = w(C) = \{P, Q\}$，代表只有主体 P、Q 可以经由信道 C 发送和接收消息。

如果要使用一个信道，一个协议的主体需要知道如何从信道读取信息和向信道发送信息，分别使用 C^r 和 C^w 表示。如果主体 P 是信道 C 消息的一个接收者，则 $P \in r(C)$，当且仅当 P 拥有 C^r。相似地，如果主体 P 是信道 C 消息的发送者，则 $P \in w(C)$，当且仅当 P 拥有 C^w。

在 PI 积分的基础上，给出以下几种信道模型：

公共信道： C 是公共信道，当且仅当系统中的任何主体可以在信道上发送和接收消息，即 $r(C) = w(C) = \Omega$，Ω 是所有协议主体的集合。

认证信道： C 是认证信道，当且仅当任何主体可以从它读取信息，但是只有主体 P 有权向这个信道发送消息，即 $r(C = \Omega)$ 并且 $w(C) = P$。认证信道可以通过使用数字签名实现。

秘密信道： C 是秘密信道，当且仅当任何实体可以向这个信道发送消息，但是只有一个主体 P 可以从信道接收消息，即 $r(C) = \{P\}$ 并且 $w(C) = \Omega$。秘密信道可以通过基于公钥的加密来实现。

专用信道： C 是专用信道，当且仅当只有主体 P 可以从这个信道接收消息，只有主体 Q 可以向这个发送消息，即 $r(C) = \{P\}$ 并且 $w(C) = \{Q\}$。专用信道可以通过组合认证信道与秘密信道的属性来实现。

闭群信道： C 是闭群信道，当且仅当一组主体可以向信道发送消息，同样的一组主体可以从信道接收消息，即 $r(C) = w(C) = \mathrm{A}$，其中 A 为一组主体的集合。可以通过使用对称密钥来实现闭群信道。

专享秘密信道： C 是常规秘密信道，当且仅当它只可以被两个主体 P 和 Q 使用，即 $r(C) = w(C) = \{P, Q\}$。

3. 逻辑实现

在众多认证协议的形式化方法中，最有影响的是 BAN 逻辑[5]，其最主要的贡献在于协议验证方面，同时衍生出 BAN 类逻辑，如 GNY 逻辑等等，目前仍然有很多学者将其应用于安全协议的分析。本文提出的逻辑与 BAN 逻辑一样也是多类型模态逻辑（many-sorted modal logic）。逻辑由语言、推理规则、分解规则等组成。语言用来描述假设和事件，以及协议的目标，推理规则和分解规则用来获得系统新的状态。同时也采用 GNY 逻辑的一些概念，尽管 GNY 逻辑被认为过分复杂且不适宜使用，但是其中的某些思想被认为是对 BAN 逻辑的巨大改进[6]。逻辑的主要目的是推理认证协议，模型了先前提到的协议中主体的行为和信道。

3.1 基本语法

假设 P、Q 代表主体，C 代表信道，X 代表消息，$C(X)$ 代表信道 C 中的消息 X，ϕ 代表公式。逻辑语言的基本语法主要有 10 个构件：

1) $P \lhd C(X)$：某个主体经由信道 C 发送了消息 X，主体 P 可以观察到。如果 P 无权从信道读取信息，则 P 无法理解这个消息；

2) $P \lhd X \mid C$：主体 P 经由信道 C 收到消息 X，即存在某个主体向 P 发送了包含 X 的消息；

3) $P \lhd X$：主体 P 收到了包含消息 X 的消息；

4) $\#(X)$:X 是新鲜的，即 X 没有在当前回合作为某消息的一部分被发送过；

5) $P \mid\sim X$：主体 P 曾经发送过包含 X 的消息；

6) $P \mid\mid\sim X$：主体 P 一定在当前回合发送过包含 X 的消息；

7) $P \mid\equiv \phi$：主体 P 相信公式 ϕ 是真的；

8) $P \mid\equiv ((Q \mid\mid\sim \phi) \rightarrow (Q \mid\equiv \phi))$ 如果主体 P 相信 Q 当前回合发送过包含 ϕ 的消息，则 Q 相信 ϕ；

9) $P \mid\equiv ((Q \mid\equiv \phi) \rightarrow \phi)$：主体 P 相信如果 Q 相信 ϕ，则 ϕ 是真的；

10) $P \mid\equiv ((Q \mid\mid\sim \phi) \rightarrow \phi)$：主体 P 相信如果 Q 这个回合发送过包含 ϕ 的消息，则 ϕ 是真的；

3.2 推理规则

推理规则主要由看见规则、解释规则、新鲜性规则组成。

1）看见规则(seeing rules)：

$\dfrac{P \lhd C(X), P \in r(C)}{P \mid\equiv (P \lhd X \mid C), P \lhd X}$：如果主体 P 经由信道 C 收到一个消息 X，并且 P 可以接收这个信道上的消息，则 P 认识到消息已经到达并且它可以理解这个消息；

$\frac{P \lhd (X,Y)}{P \lhd X, P \lhd Y}$：如果 P 收到一个合成的消息(X,Y)，则它收到消息的部分（X 和 Y）；

2）解释规则(interpretation rules)：

$\frac{P \mid\equiv (w(C) = W)}{P \mid\equiv ((P \lhd X \mid C) \to \vee_{\forall Q_i \in W \setminus \{P\}} (Q_i \mid\sim X))}$：如果主体 P 相信信道 X 仅仅可以被主体集合 W 中的主体写入数据，则 P 相信如果它经由信道 C 收到一个消息，则主体集合 W 中的某个主体说过 X；

$\frac{P \mid\equiv (Q \mid\sim (X,Y))}{P \mid\equiv (Q \mid\sim X), P \mid\equiv (Q \mid\sim Y)}$：如果 P 相信另一个主体 Q 已经说过一个组合的消息(X,Y)，则它相信 Q 相信这个消息中的部分内容；

3）新鲜性规则(freshness rules)：

$\frac{P \equiv (Q \mid\sim X), P \mid\equiv \#(X)}{P \mid\equiv (Q \mid\mid\sim X)}$：如果主体 P 相信另一个主体 Q 说过一个消息 X，并且 P 相信 X 是新鲜的，则 P 相信 Q 当前回合说过 X；

$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$：如果主体 P 相信组合消息中的部分内容是新鲜的，则它相信整个消息是新鲜的。

3.3 分解规则

以下 9 条分解规则是非常直观的，$\mapsto$ 代表后面的表达式是实现前面目标的必须条件。将协议的目标使用分解规则进行分解，如果分解后得到的结果是正确的，则协议的目标是正确的。由于篇幅原因只解释其中的几条。

1) $P \mid\equiv (P \lhd X \mid C)$ ： $\mapsto P \lhd C(X)$ ，$\mapsto P \in r(C)$：主体 P 经由信道 C 收到消息 X，则某个主体经由信道 C 发送了消息 X，主体 P 有权从信道读取信息；

2) $P \lhd X$：$\mapsto P \lhd (X,Y) / P \mid\equiv (P \lhd X \mid C)$：主体 P 收到一个消息 X，则 P 可能收到组合消息(X,Y)，或者经由信道 C 收到消息 X；

3) $P \mid\equiv (Q \mid\sim X)$：$\mapsto P \mid\equiv (Q \mid\sim (X,Y))$：P 相信 Q 说过消息 X，则 P 相信消息组合（X,Y）；

4) $P \mid\equiv (Q \mid\sim X)$ ： $\mapsto P \lhd C(X)$ ，$\mapsto P \in r(C)$ ，$\mapsto P \mid\equiv (w(C) = \{Q\}) / P \mid\equiv (w(C) = \{P,Q\})$，

$\mapsto \lhd X$：P 相信 Q 说过消息 X，则 P 经由信道 C 收到消息 X；

5) $P \mid\equiv \#(X)$：$\mapsto P \mid\equiv (X')$：P 相信 X 是新鲜的，则 P 相信 X 的部分 X' 是新鲜的；

6) $P \mid\equiv (Q \mid\mid\sim X)$ ： $\mapsto P \lhd C(X)$ ，$\mapsto P \in r(C)$ ，$\mapsto P \mid\equiv (w(C) = \{Q\}) / P \mid\equiv (w(C) = \{P,Q\})$ $\mapsto P \mid\equiv \#(X)$，$\mapsto Q \mid\equiv X$；

7) $P \mid\equiv (Q \mid\equiv \phi)$ ： $\mapsto P \mid\equiv (Q \mid\mid\sim \phi)$ ，$\mapsto P \mid\equiv ((Q \mid\mid\sim \phi) \to (Q \mid\equiv \phi))$；

8) $P \mid\equiv \phi$ ： $\mapsto P \mid\equiv (Q \mid\mid\sim \phi)$ ，$\mapsto P \mid\equiv ((Q \mid\mid\sim \phi) \to \phi)$；

9) $P \mid\equiv \phi$：$\mapsto P \mid\equiv \phi'$，$\mapsto P \mid\equiv (\phi' \to \phi)$。

4. Woo-Lam 认证协议的分析与设计

4.1 Woo-Lam 认证协议

Woo-Lam 认证协议的非形式化描述如下：

（1） $A \to B : A$；（2） $B \to A : N_b$；（3） $A \to B : \{N_b\}_{K_{as}}$；（4）$B \to S : \{A, \{N_b\}_{K_{as}}\}_{K_{bs}}$；（5） $S \to B : \{N_b\}_{K_{bs}}$。

协议中主体 A 借助于服务器 S 的帮助向主体 B 进行自我身份认证，使主体 B 确信是主体 A 与它通信。可以用本文提出的逻辑对协议进行描述如下：

（1）$B \lhd A$；（2）$A \lhd N_b$；（3）$B \lhd C_{as}(N_b)$；

（4）$S \lhd C_{bs}(A, C_{as}(N_b))$；（5）$B \lhd C_{bs}(N_b)$。

显然协议必须满足如下条件：

1. $A \in r(C_{as})$：A 可以从信道 C_{as} 接收信息；
2. $S \in r(C_{as})$：C 可以从信道 C_{as} 接收消息；
3. $A \mid\equiv (w(C_{as}) = \{A,S\})$：A 相信只有 A、S 可以在信道 C_{as} 上发送消息；
4. $S \mid\equiv (w(C_{as}) = \{A,S\}\}$：S 相信只有 A、S 可以在信道 C_{as} 上发送消息；
5. $B \in r(C_{bs})$：B 可以从信道 C_{bs} 读取消息；
6. $S \in r(C_{bs})$：S 可以从信道 C_{bs} 读取消息；
7. $B \mid\equiv (w(C_{bs}) = \{B,S\})$：B 相信只有 B、S 可以向信道 C_{bs} 发送消息；
8. $S \mid\equiv (w(C_{bs}) = \{B,S\})$：S 相信只有 B、S 可以向信道 C_{bs} 发送消息；
9. $A \mid\equiv ((S \mid\mid\sim \phi) \to (S \mid\equiv \phi))$：A 相信 S 是诚实的；
10. $A \mid\equiv ((S \mid\equiv (B \mid\sim X)) \to (B \mid\sim X))$：A 相信 S 有能力判断是否 B 说过消息 X；
11. $B \mid\equiv ((S \mid\mid\sim \phi) \to (S \mid\equiv \phi))$：B 相信 S 是诚实的；

978-1-935068-23-5 © 2010 SciRes.

12. $B \mid\equiv ((S \mid\equiv (A \mid\sim X)) \rightarrow (A \mid\sim X))$：B 相信 S 有能力判断 A 是否说过 X；

13. $B \mid\equiv \#(N_b)$：B 相信 N_b 是新鲜的。

Woo-Lam 认证协议是有安全缺陷的，其缺陷在于协议目标的失误，将协议的目标看作为 $B \mid\equiv (A \mid\sim (N_b))$，而这个安全目标不能抵抗来自内部合法主体的重放攻击，如一个合法的主体 Z 可以伪装成 A 发起一个与 B 的通信[7]。因此本文提出新的安全目标：$B \mid\equiv (A \mid\sim (B, N_b))$，表示 B 相信 A 是当前回合与它通信的主体，它在当前回合说过 (B, N_b)，(B, N_b) 中的 B 明确了通信对象，可以避免重放攻击。

4.2 协议目标分解与设计

对新的安全目标 $B \mid\equiv (A \mid\sim (B, N_b))$ 使用分解规则 5：$\mapsto B \mid\equiv (A \mid\sim (B, N_b))$；$\mapsto B \mid\equiv \#(B, N_b)$；

对 $B \mid\equiv \#(B, N_b)$ 使用分解规则 6：$\mapsto B \mid\equiv \#(N_b)$；这个结果是条件 13，因此这个目标是达到了。继续对 $B \mid\equiv (A \mid\sim (B, N_b))$ 使用分解规则 8：

$\mapsto B \mid\equiv (S \mid\sim (A \mid\sim (B, N_b)))$；

$\mapsto B \mid\equiv ((S \mid\sim (A \mid\sim (B, N_b))) \rightarrow (A \mid\sim (B, N_b)))$

由条件 11，12 知这两个新的目标达到了。继续对目标 $B \mid\equiv (A \mid\sim (B, N_b))$ 进行分析。

继续对 $B \mid\equiv (S \mid\sim (A \mid\sim (B, N_b)))$ 使用分解规则 5：$\mapsto B \lhd C_{bs}(A \mid\sim (B, N_b))$；$\mapsto B \in r(C_{bs})$；$\mapsto B \mid\equiv (w(C_{bs}) = \{B, S\})$；$\mapsto B \mid\equiv \#(A \mid\sim (B, N_b))$；$\mapsto S \mid\equiv (A \mid\sim (B, N_b))$。由条件 5，7 知，第 2 和第 3 新目标可以达到；由条件 13 知第 4 个新目标可以达到；第 1 个新目标可以经由信道 C 通过发送公式 $A \mid\sim (B, N_b)$ 来实现。

继续对 $S \mid\equiv (A \mid\sim (B, N_b))$ 使用分解规则 4：$\mapsto S \lhd C_{as}(B, N_b)$；$\mapsto S \in r(C_{as})$；

$\mapsto S \mid\equiv (w(C_{as}) = \{A, S\})$；$\mapsto A \lhd (B, N_b)$。

第一个新目标是协议的消息，由条件 2， 4 知第 2 与第 4 个新目标满足，第 4 个目标可以通过给 A 发送消息 (B, N_b) 来实现。

因此新的协议可以如下表示：

$A \lhd (B, N_b)$ ； $S \lhd C_{as}(B, N_b)$ ；

$B \lhd C_{bs}(A \mid\sim (B, N_b))$。

对于协议有不同的实现方法，这里给出一种与初始协议相似的实现方法：

$A \rightarrow B : A$ ； $B \rightarrow A : B, N_b$ ；

$A \rightarrow B : \{B, N_b\}_{K_{as}}$ ； $B \rightarrow S : A, \{B, N_b\}_{K_{as}}$ ；

$S \rightarrow B : \{A, B, N_b\}_{K_{bs}}$

而这种改进后的协议已经被证明是安全的[7]。因此可以看出采用这种方法可以设计出符合安全目标的安全协议。

5. 小结与展望

本文在 BAN 与 GYN 逻辑的基础上提出了一种简单逻辑，并将信道的概念引入其中，大大简化了逻辑，使新逻辑的推理规则少于 6 条，而且新逻辑更加清楚，可以涵盖认证协议的所有方面。通过这种方法，可以表达主体之间的信任关系。在这种逻辑的基础上，提出了一套分解规则用于认证协议的设计，以 Woo-Lam 协议为例，介绍了如何使用本文提出的逻辑与合成规则在高的抽象级别进行认证协议的设计而不必考虑细节问题。

总的来说，如果从安全协议的设计阶段就开始应用形式化的方法，设计出的协议将更加有效。在协议设计的早期阶段，不必考虑协议的具体实现细节，而要应用抽象程度较高的模型，如文中提出的简单逻辑对协议的安全目标进行分析，确定协议中每个消息所起的作用。然后确定协议中消息的结构，最后在安全协议的实现阶段可以应用抽象程度比较低的模型，这也是下一步要进行的工作。

致谢

感谢解放军理工大学肖军模教授提供的大力帮助。

References (参考文献)

[1] FAN Hong, Feng Deng-guo, security protocol theory and method, Beijing: Science Press,2003.
范红，冯登国，安全协议理论与方法，北京：科学出版社，2003。

[2] LIU Jing, Fu Fei, Formal Analysis Model of Secure Routing Protocols for Ad Hoc Networks, Journal of PLA University of Science and Technology(Natural Science Edition) , 2008, Vol.9（3）
刘晶，伏飞, Ad Hoc网络安全路由协议形式化分析模型[J]，解放军理工大学学报，2008, Vol.9（3）.

[3] FU Fei, Secure Routing Protocol for Ad hoc Networks, Journal of University of Electronic Science and Technology of China，2009， Vol.38（3）。

伏飞,新的 Ad hoc 网络安全路由协议[J]，电子科技大学学报，2009,Vol.38（3）。

[4] M.Abadi and A. D. Gordon. A calculus for cryptographic protocols:The spi calculus.In Proceedings of the 4th ACM Conference on Computer and Communications Security.pages 36-47,1997.

[5] A Logic of Authentication, M.Burrows, M. Abadi and R. Needham,ACM Transactions on Computer Systems, v8n1, February 1990.

[6] L. Gong, R. Needham,and R. Yahalom. Reasoning about belief in cryptographicprotocols.In Proceeding of the 1990 IEEE Computer Symposium on Research in Security and Privacy.IEEE Cpmputer Society Press,Los Alamitos,California,234-248,1990.

[7] M. Abadi and R. Needham.Prudent engineering practice for cryptographic protocols.In Proceedings of the IEEE CS Symposium on Research in Security and Privacy,pages 122-136, 1994.。

978-1-935068-23-5 © 2010 SciRes.