Kailar 逻辑的改进及应用*

翁艳琴[1,2],石曙东[1],解颜铭[1,2]
(1.湖北师范学院 数学与统计学院,湖北 黄石 435000;
2.湖北师范学院 计算机科学与技术学院,湖北 黄石 435000)

摘 要:综合 Kailar 逻辑和 SVO 逻辑两种协议分析方法的优点,借助 SVO 逻辑的思想对 Kailar 逻辑进行了改进,使其更好地应用于不可否认协议的可追究性分析和设计。同时,将改进后的 Kailar 逻辑应用在类 NG 协议的分析中,分析结果证明了该协议可追究方面的安全性质。

关键词:逻辑系统;Kailar 逻辑;SVO 逻辑;安全协议
中图分类号:TP309 **文献标识码**:A **文章编号**:1674-7720(2012)03-0056-03

The extension and application of Kailar logic

Weng Yanqin[1,2], Shi Shudong[1,2], Xie Yanming[1,2]
(1.Institute of Mathematics and Statistical, Hubei Normal University, Huangshi 435000, China;
2.Institute of Computer Science and Technology, Hubei Nomal University, Huangshi 435000, China)

Abstract: This paper sums up the advantages of Kailar logic and SVO logic, extends Kailar logic with the help of the ideas of SVO logic to make it better for the undeniable agreement analysis and design. At the same time, by applying the expanded Kailar logic to analyze the class NG agreement, the result proves that the agreement is safe in the accountability nature.

Key words: logical system; Kailar logic; SVO logic; security protocol

协议的安全性分析在安全协议的设计中起着重要的作用,Kailar 逻辑的提出主要是针对电子商务协议的可追究性,但它不能分析签名的密文,对协议的证明不严格。SVO 逻辑也可用于电子商务协议的形式化分析,它集成了 BAN、GNY、AT 等逻辑的优点,具有很好的扩展能力。本文针对 Kailar 逻辑的不足,借助 SVO 逻辑的分析思想对 Kailar 逻辑进行了改进和完善,使得新的 Kailar 逻辑能分析签名密文,严格推证协议是否具有不可否认性。

1 Kailar 逻辑的基本架构

Kailar 逻辑的基本架构包含基本语句、分析假设和推理原则,限于篇幅,本文只对涉及的语句、推理原则进行说明,其他的不一一列举。

(1)基本语句 A,B,C……为参与协议的主体,通常用 P 指代。TTP 专指可信的第三方。m 为一个主体给另一个主体发送的原子消息。C 为原子消息外的消息。K_i 为主体 i 的公开密钥。K_i^{-1} 为与 K_i 对应的秘密私钥。x,y……为命题。

(2)基本推理原则为以下 3 个:

(P1) A Says m⇒A Sent m

(P2) $\dfrac{\text{A Can prove x; x}\Rightarrow\text{y}}{\text{A Can prove y}}$

(P3) $\dfrac{\text{A Can prove x; A Can prove y}}{\text{A Can prove}(\text{x}\wedge\text{y})}$

2 可追究原则的改进

本文假定发送者为 A,接收者为 B,可信第三方为 TTP,其他符号含义同上。在 Kailar 逻辑中,只是涉及了接收方对发送方的主体签名的追究性,没有涉及发送方对接收方的签名的追究性,同时对第三方 TTP 对参与协议的其他方的追究性也没有明确的推理规则。本文借助 SVO 逻辑的思想,对 Kailar 逻辑进行了完善,改进后的推理原则如下:

(1)发送方的签名追究性

两方间:(P4) $\dfrac{\text{B Can prove}(K_p\ \text{Authenticates A})}{\text{B Can prove}(\text{A says m})}$ B Received(m Signedwith K_p^{-1});

*基金项目:湖北省自然科学基金(2006ABA056);湖北省教育厅重点项目(D20092203);湖北省教育厅青年项目(Q20102503)

$$\text{三方间：(P5)}\ \frac{\begin{array}{c}\text{B Believe TTP;}\\ \text{TTP Can prove(A Says C)}\end{array}}{\text{B Can prove(A Says C)}}$$

$$\text{(P6)}\ \frac{\begin{array}{c}\text{A Believe TTP;}\\ \text{TTP Can prove(B Received C)}\end{array}}{\text{A Can prove(B Received C)}}$$

$$\text{(P7)}\ \frac{\begin{array}{c}\text{TTP Received m Signedwith K AT;}\\ \text{Shared (A, K AT ,TTP)}\end{array}}{\text{TTP Can prove(A says m)}}$$

(2)接收方的签名追究性

两方间：

$$\text{(P8)}\ \frac{\begin{array}{c}\text{A Can prove(B Received m Signedwith } K_x^{-1}\text{);}\\ \text{A Can prove(B Received } K_x\text{)}\end{array}}{\text{A Can prove(B Received m)}}$$

$$\text{(P9)}\ \frac{\begin{array}{c}\text{B Can prove(A Says m Signedwith } K_x^{-1}\text{);}\\ \text{B Can prove (A Says } K_x\text{)}\end{array}}{\text{B Can prove(A Says m)}}$$

$$\text{(P10)}\ \frac{\begin{array}{c}\text{A Can prove(B Says C);}\\ \text{A sent(Np}\wedge\text{C);A Received(Np'}\wedge\text{C)}\end{array}}{\text{A Can prove(B Received C)}}$$

三方间：

$$\text{(P11)}\ \frac{\begin{array}{c}\text{TTP Received (C Signedwith } K_{BT}\text{);}\\ \text{Shared(B,}K_{BT}\text{,TTP);TTP Can prove(A says C)}\end{array}}{\text{TTP Can prove(B Received C)}}$$

信任规则：

$$\text{(P12)}\ \frac{\text{B Can prove(A Sent m)}}{\text{B Believe (A Sent m)}}$$

$$\text{(P13)}\ \frac{\text{A Can prove(B Received m)}}{\text{A Believe (B Received m)}}$$

接收规则：

$$\text{(P14)}\ \frac{\text{P Received (x,y) Signedwith } K^{-1}}{\begin{array}{c}\text{P Received(x)Signedwith } K^{-1}\\ \text{OR P Received (y) Signedwith } K^{-1}\end{array}}$$

3 应用 Kailar 逻辑进行协议分析

不可否认协议(类 NG 协议)的交互过程如图 1 所示。

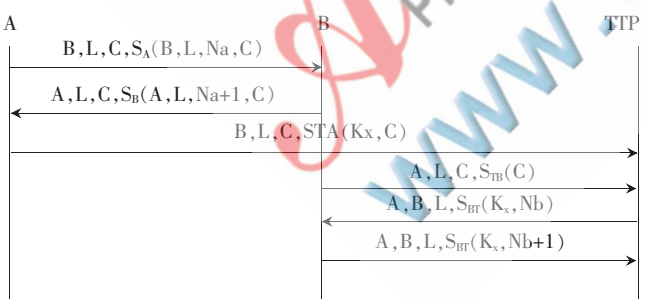

图 1 类 NG 协议交互图

图 1 中的符号含义为：A、B 为协议参与双方，TTP 为可信第三方。L 为协议轮标志。Na、Nb 为新的随机数。S_A、S_B 为 A、B 的私钥。S_{AT}、S_{BT} 分别为 A、T 间共享密钥，B、T 间共享密钥。K_x 为 A 产生的消息密钥。$C=(m)K_x^{-1}$，m 为发送的消息原语。此协议中 A 发送给 B 一个由 K_x 加密的消息 C 后通过第三方 TTP 传递 K_x 给 B。此协议具有实现 A、B、TTP 间的消息可追究性的性质。

(1)协议的前提和假设

假设 1：A Can prove(K_B Authenticates B)；

假设 2：B Can prove(K_A Authenticates A)；

假设 3：Shared(A, K_{AT}, TTP)；

假设 4：Shared(B, K_{BT}, TTP)；

假设 5：A Believe TTP；

假设 6：B Believe TTP。

(2)说明协议目标

G1：A Believe(B Received m)；

G2：B Believe(A Sent m)；

G3：TTP Believe(A Sent m)；

G4：TTP Believe (B Received m)。

(3)运用规则和公理进行推证协议理想化描述为：

(M1)B Received((B, L, Na, C)Signedwith K_A^{-1})

(M2)A Received((A, L, Na+1, C)Signedwith K_B^{-1})

(M3)TTP Received((Kx, C)Signedwith K_{AT})

(M4)TTP Received(C Signedwith K_{BT})

(M5)B Received((Kx, Nb)Signedwith K_{BT})

(M6)TTP Received((Kx, Nb+1)Signedwith K_{BT})

(4)协议分析

①由协议描述(M2)知 A Received(C Signedwith K_B^{-1})(规则 P14)。结合假设 1 可得结论 1：A Can prove(B Says C)(规则 P4)。由原则 P1 和 P2 可得结论 2：A Can prove(B Sent C)。再结合已知 A Sent(Na∧C)和 A Received(Na'∧C)，根据原则 P10 可得结论 3：A Can prove(B Received C)。其中，$C=(m)K_x^{-1}$，即有结论 4：A Can prove(B Received m Sighned with K_x^{-1})。

由协议描述(M6)知 TTP Received((Kx)Signedwith K_{BT})(规则 P14)，而由假设 4，基于原则 P6 有结论 5：TTP Can prove(B Says Kx)，根据原则 P1 和 P2 有结论 6：TTP Can prove(A Sent Kx)。由结论 6 结合已知 TTP Sent(Nb∧Kx)和 TTP Received(Nb'∧Kx)，运用原则 10 可得出结论 7：TTP Can prove(B Received Kx)，结合假设 5 和结论 7，运用原则 P6 可得结论 8：A Can prove(B Received Kx)。结合结论 4，应用原则 P8 可推出结论 9：A Can prove (B Received m)，进而应用原则 P13 可得结论 10：A Believe(B Received m)，此结论即为要达成的协议目标 G1。

②由协议描述(M1)基于规则 P14 知 B Received(C Signedwith K_A^{-1})，而由假设 2，运用原则 P4 可得结论 11：B Can prove(A says C)，进一步运用原则 P1 和 P2 可得结论 12：B Can prove (A Sent C)，而 $C=(m)K_x^{-1}$，即有结论 13：B Can prove(A Sent m Sighned with K_x^{-1})。

由描述(M3)知 TTP Received(K_x Signedwith K_{AT})，结合假设 3 和规则 P4 有结论 14：TTP Can prove(A Says Kx)，进一步结合假设 6，应用规则 P5 有结论 15：B

Can prove(A Says K_x)。而结论 11 为 B Can prove(A says C)，即 B Can prove (A Says m Sighned with K_x^{-1})，应用原则 P9 可得结论 16：B Can prove(A Says m)。进一步根据原则 P1 和 P2 有结论 17：B Can prove (A Sent m)，再根据原则 P12 可得结论 18：B Believe (A Sent m)。该结论即为要达成的协议目标 G2。

③基本推理规则 P14，由协议描述 (M3) 知 TTP Received(C Signedwith K_{AT})，结合假设 3 和规则 P7 有结论 19：TTP Can prove (A Says C)，而已有结论 14 为 TTP Can prove(A Says K_x)，已知 $C=(m)K_x^{-1}$，故由 P9 可得结论 20：TTP Can prove(A Says m)，进一步应用 P1 和 P2 原则有结论 21：TTP Can prove (A Sent m)，再基于原则 P12 可得结论 22：TTP Believe(A Sent m)。结论 22 即为要达成的目标 G3。

④由协议描述(M4)、假设 4、结论 19 和原则 P11 可得结论 23：TTP Can prove (B Received C)，结合已知 $C=(m)K_x^{-1}$ 和结论 7，基于原则 P8 可得结论 24：TTP Can prove (B Received m)，进一步基于基本推理原则 P13 得出结论 25：TTP Believe(B Received m)，结论 25 即为要达成的目标 G4。

由上述分析可知，该协议的 4 个目标都可满足，协议的各方的信任都可以建立，具有不可否认的性质，协议具有追究性。

基于推理结构性方法体系通常由一些命题和推理公理组成，命题表示了主体对消息的信仰或知识，运用推理公理可以从已知的知识和信仰推导出新的知识和信仰。其中，Kailar 逻辑和 SVO 逻辑是最重要的两种方法，各具优点和不足。针对 Kailar 逻辑的不足，本文借助 SVO 逻辑的思想对其进行了改进和完善，使得它能更好地应用于协议的不可否认性和可追究性的分析。将扩展了的 Kailar 逻辑应用于类 NG 协议的可追究性的分析，证明了该协议可追究方面的安全性质。该协议分析方法简单、语义明确，为电子商务类协议的分析提供了强有力的工具。但是还有一些需要改进的地方，例如如何应用它来分析协议的公平性，如何引入恰当的初始化假设等。

参考文献

[1] 范红，冯登国.安全协议形式化分析的研究现状与有关问题[J].网络安全技术与应用，2001(8)：12-15.

[2] KAILAR R. Accountabitity in electronic commerce protocols [J]. IEEE Transactions on Software Engineering, 1996,22(5):313-328.

[3] ZHEN J, GOLLMANN D. A fair non-repudiation protocol[J]. IEEE Computer Society Symposium on Research in Security and Privacy,1996.

[4] 范红，冯登国.安全协议理论与方法[M].北京：科学出版社，2003.

[5] ZHOU J, GOLLMAN D. A fair non-repudiation protocol[C]. Proceeding of 1996 IEEE Symposium on Security and Privacy, 1996:55-61.

[6] 周典萃，卿斯汉，周展飞.Kailar：逻辑的缺陷[J].软件学报，1999，10(12)：1238-1245.

[7] 卿斯汉，常晓林，章江.安全电子商务协议 iKP I 的设计和实现[C].信息和通信安全——CC ICS'99：第一届中国信息和通信安全学术会议，2000.230-239.

[8] ISO/IEC 1388822, Information technology security techniques non-repudiation part2: mechanisms using symmetrical techniques[S]. International Organization for Standardization, 1998.

（收稿日期：2011-10-15）

作者简介：

翁艳琴，女，1985 年生，硕士研究生，主要研究方向：计算机应用和网络信息安全。

石曙东，男，1963 年生，博士，教授，主要研究方向：网络与信息安全。

解颜铭，女，1987 年生，硕士研究生，主要研究方向：信息安全。