维普资讯 http://www.cqvip.com

模型检测技术和密码协议分析*)

Model Checking and Cryptographic Protocol Analysis

张玉清　吴建平　李　星

(清华大学信息网络工程研究中心　北京 100084)

Abstract　Model checking can aid the design, analysis, and verification of the cryptographic protocols used over open networks and distributed systems. In this paper we give a survey of the state of model checking to the analysis of cryptographic protocols. We attempt to outline some of the major threads of research in this area, and also to make a suggestion of future work. These conclusions will facilitate the development of using model checker for analysis of cryptographic protocols.

Keywords　Model checking, Cryptographic protocol, Formal methods

1　引言

密码协议是建立在密码体制基础上的一种交互通信的协议，它运行在计算机通信网或分布式系统中，借助于密码算法来达到密钥分配、身份认证等目的。目前密码协议已广泛应用于计算机通信网与分布式系统中，但密码协议安全性的论证仍是一个悬而未决的问题。九十年代以来，密码协议的形式化分析成为国际上的研究热点。这种方法的出发点是希望将密码协议形式化，而后借助于人工推导，甚至计算机的辅助分析，来判别密码协议是否安全可靠。早先的密码形式分析方法采用基于信仰的逻辑——BAN 逻辑[1]，来说明和验证密码协议。随后学者们经过研究，发现 BAN 逻辑在理想化步骤等方面存在着不可逾越的障碍[2,3]，从而各国学者开始陆续尝试运用其它形式方法来分析密码协议的安全性。

众所周知，模型检测技术原是用于分析和模拟硬件工作过程的形式方法，随着形式方法的日益进步和应用领域的推广，模型检测现已用于软件分析和通信协议模拟等多个领域，但用于密码协议的分析还是这几年新的应用。

在 1996 年，英国学者 Gavin Lowe 首先启用 CSP 和模型检测技术对密码协议进行分析[4]。通信顺序进程 CSP(Communicating Sequential Processes)原是著名计算机科学家 C. A. R. Hoare 为解决并发现象而提出的代数理论[5]。在文[4]中，Gavin Lowe 采用 CSP 模型和 CSP 模型检测工具 FDR(故障偏差精炼检测器，Failures Divergences Refinement Checker)，来分析 Needham-Schroeder 公钥协议，并成功地找到一个以前从未发现的攻击。

模型检测技术应用于密码协议分析的成功，使学者们相继投入到这个领域。自 97 年起，计算机科学家及密码学家开始陆续应用模型检测这种新的形式方法来分析密码协议的安全性[6~8]。基于这种背景笔者也开始了这方面的研究，并首先启用 SMV(Symbolic Model Verifier)[9]这种新的模型检测工具软件分析了若干密码协议，取得了一些成果[10,11]。

实践证明：对于密码协议分析来讲，模型检测确实是一条非常成功的途径。

2　模型检测分析协议方法

2.1　分析基本方法

模型检测主要用于有限状态系统的分析，这就要求研究如何为密码协议构造有限状态系统。目前，模型检测分析密码协议的基本方法主要采用英国学者 Gavin Lowe 研究的最新成果[12]，即：构造一个运行协议的小系统模型(通常是一个有限状态转换系统)，同时结合一个通常意义下的入侵者模型，它能与协议交互作用，利用状态探测工具来发现系统是否进入一个不安全状态，也就是说是否对协议存在一个攻击。

这种方法发现了密码协议许多以前未发现的新攻击，极大地促进了密码协议分析与设计的研究工作。

*)本文得到国家 863 项目(No. 863-306-ZD08-01-3)基金资助。张玉清　讲师，博士后，主要研究 网络安全，电子商务，软件工程；吴建平　教授，博导，主要研究：网络体系结构，网络协议测试，形式化理论与方法；李　星　教授，博导，主要研究：高速网，网络安全，网络行为学。

维普资讯 http://www.cqvip.com

2.2 分析假设

(1)密码协议的基本假设

①加密部分从文字形式上是可以区分的。这意味着一个主体接受到一个加密项就知道这个加密项属于哪个消息,是消息的哪一部分。这个条件非常容易满足,例如只要在每个加密项中放入编号即可。

②身份可确定性。参与协议运行的所有主体的身份是可以通过协议运行中的加密项来推断的。这样对于一个主体来说,当他接受了一个加密项后,他自己就可以判断出这个加密项是否是发给他的。更进一步,如果这个加密项起源于一个诚实的主体,接受者可以判断出谁是加密项的产生者,谁是这个加密项的接受者。

假设①、②容易满足,只要在每个加密项中明显包含每个主体的身份即可;换句话说,也可以通过加密操作所运用密钥的类别——公钥、私钥或对称密钥来推断出来。

要说明的是,以上这两个假设正好是文[13]中的设计准则 11 和 3。众所周知,这些准则有效地避免了许多攻击,并且也使密码协议更容易分析。

③协议运行不用协议运行期间所建立的任何临时秘密。如果一个特别的数据项不是那种要保持为秘密的数据项,那么一个监视通信的第三者就能够从有该数据项参与的运行中获知此数据项的值(或者这个值是公共信息,第三者早已知道它),更进一步,如果一个特别的密钥不是那种要保持为秘密的密钥,那么一个监视通信的第三者就能够通过有该密钥的逆所参与的运行中获知此密钥的数值(或者明显得到,或者通过加密某些数据项)。

(2)模型假设

①完善保密假设。协议采用的密码系统是完美的,不考虑密码系统被攻破的情况等。

②入侵者的知识和能力假设。·可窃听及中途拦截系统中传送的任何消息;·可解密用他自己加密密钥(公开密钥或对称密钥)加密的消息;·在系统中可插入新的消息;·即使不知道加密部分的内容,也可重放他所看到的任何消息(其中可改变明文部分);·可运用他知道的所有知识(如临时值等),并可产生新的临时值等。

2.3 一些结论

(1)小系统的定义 参与协议运行的各主体都是唯一的(例如,一个初始者,一个响应者),作用也是唯一的。这些主体也都是诚实的:它们严格按照协议规定和遵循自己的身份参与协议运行,并不与入侵者运行协议。

这样我们在构造一个密码协议的小系统,从而应用有限状态模型检测时,必须对下列一些参数在系统中进行说明:①参与协议运行的诚实主体的个数;②每个诚实主体所起的作用;③每个诚实主体所能运行协议的次数;④入侵者的初始知识等。

(2)安全性破坏定义

定义 1(强安全性破坏) 一个诚实的主体相信在协议运行中用到的一个值是仅他和另外诚实主体之间的共享秘密,但入侵者知道这个值。

定义 2(一般安全性破坏) 一个诚实的主体相信在一个完整协议运行中用到的一个值是仅他和另外诚实主体之间的共享秘密,但入侵者知道这个值。

目前,对于模型检测技术分析密码协议,有以下已被证明的理论结果:

如果在小系统上没有对协议的攻击导致强安全性破坏,那么在任意系统上一定没有攻击导致强安全性破坏,当然也就没有攻击导致一般安全性破坏。

即:只要对被分析的密码协议在小系统上进行强安全性破坏分析,就可以保证协议在任意系统上的安全性。这大大减少了密码协议分析的工作量,并从理论上保证了人们对协议分析结果的信心。

这个理论结果极大地促进了模型检测技术在密码协议分析领域的广泛应用,使密码协议形式分析方法的主流从逻辑方法转向了模型检测,进而使密码协议的形式分析史上一层楼。

3 模型检测的现状及问题

对于协议分析来讲,模型检测已经证明是一条非常成功的途径。这种方法发现了协议的许多以前未发现的新的攻击,并提供了一套翔实的理论基础。但模型检测仍然存在着一些问题,这些问题也正是我们下一步要重点研究的问题,它们是:

(1)现有方法是否做到了理论上所要求的强安全性破坏分析?

(2)如何评价和衡量不同的检测方法和工具?

(3)目前模型检测的理论结果还不能对以下种类的密码协议进行分析,这限制了可分析协议的种类:

①协议中,某个主体接受到一个加密消息,但他无法解密该消息,只是将它传递给第三者。例如下面的密钥分配协议:

消息 1 $A\rightarrow B: A, \{N_a, A\}_{K_{as}}$

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

消息 3 $S\rightarrow A: \{K_{ab}, B\}K_a, \{N_a, N_b, \{K_{ab}, A, N_b\}_{K_{bs}}\}_{K_{as}}$

消息 4 $A\rightarrow B: \{K_{ab}, A, N_b\}_{K_{as}}, \{N_b\}_{K_{ab}}$

对于主体 B,他在消息 1 中接受的$\{N_a, A\}_{K_{as}}$就无法解密,他只是在消息 2 中将它传递给第三者 S,这样的协议模型检测技术还无法分析。

维普资讯 http://www.cqvip.com

②非标准的加密方式，即加密方式是除公开密钥和对称密钥加密外的其他加密方式。如 Hash 函数等。

③消息中包含长期秘密项，如主体的私钥。

我们将用于若干次密码协议运行的数据项，如主体的公开密钥、秘密密钥等定义为长期项；而将主体在一次协议运行中引入的临时数据项，如一次性随机数、短期密钥等定义为短期项。长期项和短期项是不同类型的数据项。若协议消息中包含主体私钥这样的长期秘密项，目前所得到的模型检测技术的理论结果，也无法分析这种密码协议的安全性。

结束语 模型检测技术分析密码协议，开启了模型检测技术新的应用领域，并且取得了公认的成功，并使密码协议的形式分析跨越了 BAN 类逻辑所存在的缺陷，向前进了一大步。但模型检测技术分析密码协议仍然存在着不少问题，这些问题仍然有待于我们继续进行研究。目前关键的问题在于模型检测只能分析有限状态系统，这势必对可以分析的密码协议有所要求。未来的研究趋势是如何扩大模型检测技术可分析密码协议的种类并和定理证明技术相结合，从而扩大可分析密码协议的种类，进而解决密码协议安全性分析问题。

参 考 文 献

1 Burrows M, Abadi M, Needham R. A Logic of Authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18～36

2 Boyd C, Mao W. On a Limitation of BAN Logic. In: EUROCRYPT'93. Berlin: Springer-Verlag, 1993. 240～247

3 张玉清，李继红，肖国镇. 密码协议分析工具——BAN 逻辑及其缺陷. 西安电子科技大学学报, 1999, 26(3): 376～378

4 Lowe G. Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR. In: Proc. of TACAS'96. Berlin: Springer Verlag, 1996. 147～166

5 Hoare C A R. Communicating Sequential Processes. Prentice-Hall, 1985

6 Dang Z, Kemmerer R. Using the ASTRAL Model Checker for Cryptographic Protocol Analysis. In: DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997. Available at URL: http://dimacs.rutgers.edu/Workshops/Security/program2/program.html

7 Marrero W, Clarke E, Jha S. A Model checker for Authentication Protocols. In: DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997. Available at URL: http://dimacs.rutgers.edu/Workshops/Security/program2/program.html

8 Mitchell J, Mitchell M, Stern U. Automated Analysis of Cryptographic Protocols using Murφ. In: Proc. of the IEEE Symposium on Security and Privacy. USA: IEEE Computer Society Press, 1997. 141～151

9 SMV. Available at: URL. http://www.cs.cmu.edu/~modelcheck/

10 Zhang Yuqing, Xiao Guozhen. Breaking and fixing the Helsinki protocol using SMV. ELECTRONICS LETTERS, 1999, 35(15): 1239～1240

11 张玉清，王磊，肖国镇，等. Needham-Schroeder 公钥协议的模型检测分析. 软件学报, 2000, 11(10): 1348～1352

12 Lowe G. Towards a Completeness Result for Model Checking of Security Protocols. Journal of Computer Security, 1999, 7(2～3): 89～146

13 Abadi M, Needham R. Prudent Engineering Practice for Cryptographic Protocols. IEEE Transactions on Software Engineering, 1996, 22(1): 6～15

（上接第 125 页）

1）对于 S 蕴涵 $S(1-a,b)$，不是对于所有的 S 范数都满足信息度约束，如 $S(a,b)=a+b-ab$ 就不能使 S 蕴涵满足信息度约束。

表 1 不同蕴涵运算的信息度约束分析

蕴涵算子	种类	是否满足信息度约束
a(1-|b-a|)	约束蕴涵	否
b^a	A 蕴涵	是
Min(a,b)	T 范数	是
ab	T 范数	是
max(1-a,b)	S 蕴涵	是
1-a+b-(1-a)b	S 蕴涵	否
min(1,b/a)	R 蕴涵	否
min(1,1-a+b)	R 蕴涵	是

2）不是对于所有的 R 蕴涵都满足信息度约束。

3）T 范数 Min 运算虽然与二值蕴涵运算不相容，但由于其满足信息度约束，因此在实际应用中通常用 Min 运算作为蕴涵运算而能得到较好的性质。

结论 本文利用 Yager 的特征测度，推出了在基于推理合成算法的模糊推理中，模糊蕴涵运算满足信息度约束的条件。在选用模糊蕴涵运算时，应从模糊子集的角度考虑它的信息度约束，而不只局限于模糊蕴涵运算在定义域上单点处的性质。

参 考 文 献

1 Yager R. R. Measures of information in Generalized constraints. Int. j. uncertainty, fuzziness and knowledge-based systems, 1998, 6: 519～532

2 Fernandez F G, Kreinovich V. Fuzzy Implication Can be Arbitrarily Complicated: A Theorem. Int. J. Intelligent Systems, 1998, 13: 445～451

3 Turksen I B, Kreinovich V, Yager R R. A new class of fuzzy implications. Axioms of fuzzy implication revisited. Fuzzy Sets and Systems, 1998, 100: 262～272

4 陈丹，何华灿，王晖. 模糊蕴涵和模糊推理研究. 计算机科学, 2000. 7

5 Dujet C, Vincent, N. Force implication: A new approach to human reasoning. Fuzzy Sets and Systems, 1995, 69: 53～63

6 Yager R R. Default knowledge and measures of specificity. Information Sciences, 1992, 61: 1～44

7 Yager R R. On the global requirement for the implication operators in fuzzy modus ponens. Fuzzy Sets and Systems, 1993, 106: 3～10

8 Klir G J, Bo Y. Fuzzy Sets and Fuzzy Logic: Theory and Application, Prentice-Hall, NJ, 1995