# 802.11i的认证安全性分析

邓淼磊[1] 周跃华[2] 余 涛[2] 周利华[1]

(西安电子科技大学计算机学院 西安 710071)[1] (解放军信息工程大学理学院 郑州 450001)[2]

**摘 要** IEEE设计802.11i协议解决无线局域网的安全问题。802.11i协议的形式化分析,对于确保该协议的正确性至关重要。利用串空间理论对802.11i协议进行建模,在串空间模型中验证协议的认证属性。结果表明,802.11i协议能够安全实现它的认证功能。

**关键词** 802.11i,安全协议,串空间,认证

## Authentication Analysis of the IEEE 802.11i

DENG Miao-lei[1] ZHOU Yue-hua[2] YU Tao[2] ZHOU Li-hua[1]

(College of Computer Science, Xidian University, Xi'an 710071, China)[1]

(Institute of Science, PLA Information Engineering University, Zhengzhou 450001, China)[2]

**Abstract** IEEE 802.11i protocol is used in resolving the security issues in wireless local area networks. Formal verification of 802.11i protocol is very important to guarantee the correctness of this protocol. 802.11i protocol was modeled using the strand space theory, and the authentication property of the resulting model was verified. Analysis proves that the authentication of 802.11i is not compromised in the presented model.

**Keywords** 802.11i, Security protocol, Strand space, Authentication

## 1 引言

无线局域网络由于其简单的设备安装与维护、方便快捷的接入方式以及越来越高的接入速度,正在获得日益广泛的应用。但是,无线局域网络的物理开放特性使其容易受到攻击,因而保证数据安全成为无线局域网络最重要的问题之一。为了提高无线局域网的安全性,在IEEE802.11协议中采用了WEP作为其基本的安全措施。但由于设计上的缺陷,该协议存在安全漏洞,已经严重威胁到无线局域网标准的进一步应用。IEEE802.11i[1]致力改进相关问题,它主要从认证与加密两个方面来加强无线局域网络的安全性。在认证方面,802.11i使用了IEEE802.1x,EAP和动态密钥管理,提供了双向认证和密钥管理功能。

本文的重点在于利用形式化分析安全协议的串空间模型[2],对802.11i协议的认证进行安全性分析。串空间模型是建立在Dolev-Yao模型基础上的形式化分析安全协议的著名工具,被广泛用于验证各类协议的安全性[3-5]。串空间模型把协议的描述和目标安全属性都转化为图的结构,有利于借助图的理论和算法。在分析过程中,使用了推理技术,避免了状态爆炸问题。分析过程简洁、直观、精确。

## 2 串空间模型

一个串就是协议参与者(主体)的事件序列,对于一个合法主体,它表示在协议的一次运行中主体的行为,称为正常串。入侵者串是入侵者可能发送和接收的消息序列,它模拟入侵者的能力。设$A$是协议执行中所有可能消息的集合,称$A$的元素为项。$t_1 \sqsubset t$表示$t_1$是$t$的子项。在协议中,主体可以接收或发送项。项以带正号的形式出现时表示发送消息,以带负号的形式出现时表示接收消息。

**定义1** 一个有符号项是一个二元组$\langle \sigma, a \rangle$,其中$a \in A$,$\sigma$是正号或负号。

这样可以把一个项$t$记为$+t$或$-t$。$(\pm A)^*$表示全体有符号项的有限序列的集合。

**定义2** A上的一个串空间是一个串的集合$\Sigma$,存在一个迹的影射$tr: \Sigma \rightarrow (\pm A)^*$。

**定义3** 对于一个串空间$\Sigma$,

1)结点是一个序偶$\langle s, i \rangle$,其中$s \in \Sigma$,$i$是满足$1 \leqslant i \leqslant \text{length}(tr(s))$的整数。$N$表示结点的集合。称结点$n = \langle s, i \rangle$属于串$s$或在串$s$上,记作$n \in s$。正常串上的结点称为正常结点。

2)如果$n = \langle s, i \rangle \in N$,用index$(n)$表示$n$在$s$上的索引,那么index$(n) = i$。定义项$(n)$为$s$上第$i$个有符号项。

3)如果$n_1, n_2 \in N$,那么$n_1 \rightarrow n_2$表示项$(n_1) = +a$,项$(n_2) = -a$,即$n_1$发送消息$a$,这个消息被$n_2$接收。

4)如果$n_1, n_2 \in N$,那么$n_1 \Rightarrow n_2$表示$n_1, n_2$出现在同一个串上,$n_1$是$n_2$的直接前继。

5)无符号项$t$在$n \in N$发生,当且仅当$t \sqsubset$项$(n)$。

6)无符号项$t$在$n \in N$生成,当且仅当项$(n)$的符号为正,$t \sqsubset$项$(n)$,而且对于同一串上$n$的任意前继结点$n'$,有$t \not\sqsubset$项$(n')$。

7)无符号项$t$是唯一生成的,当且仅当$t$生成在唯一的结点$n \in N$。

8)结点以及结点间的关系$\Rightarrow$和$\rightarrow$构成了一个有向图。

**定义4** 设$C$是一个有向图,$C$中有两种边$\Rightarrow$和$\rightarrow$,$N_C$是$C$的结点集合,$C$是一个丛,如果满足:

1)$C$是有限的;

**邓淼磊** 博士生,讲师,主要研究领域为信息安全;**周跃华** 讲师,主要研究领域为光信息科学;**余 涛** 硕士生,主要研究领域为信息安全;**周利华** 博士,教授,博士生导师,主要研究领域为计算机网络安全理论与技术。

2)如果 $n_1 \in N_C$，且项$(n_1)$是负的，那么存在唯一的结点 $n_2$，使得 $n_2 \rightarrow n_1 \in C$；

3)如果 $n_1 \in N_C$，且 $n_2 \Rightarrow n_1$，那么 $n_2 \Rightarrow n_1 \in C$ 并且 $n_2 \in C$；

4)$C$ 是无环的。

**定义 5** $n \in N_C$，$n$ 在丛 $C$ 中，记作 $n \in C$；如果一个串 $s$ 的所有结点都在 $N_C$ 中，那么称 $s$ 在丛 $C$ 中。串 $s$ 的丛高是使得 $\langle s,i \rangle \in C$ 的最大 $i$ 值。

入侵者的密钥集记为 $K_P$，它包括所有公钥、入侵者的私钥、入侵者和其他主体共享的对称密钥、丢失或破解的密钥等。

**定义 6** 入侵者串的迹是下列形式之一：

$M$ 发送：$\langle +t \rangle$；

$F$ 截获：$\langle -g \rangle$；

$T$ 转发：$\langle -g,+g,+g \rangle$；

$C$ 级联：$\langle -g,-h,+gh \rangle$；

$S$ 拆分：$\langle -gh,+g,+h \rangle$；

$K$ 密钥：$\langle +K \rangle$，这里 $K \in K_P$；

$E$ 加密：$\langle -K,-h,+\{h\}_K \rangle$；

$D$ 解密：$\langle -K^{-1},-\{h\}_K,+h \rangle$。

具有上述形式迹的串分别称作 $M$ 串、$F$ 串等。入侵者串上的结点称为入侵者结点。

**公理** 1(自由加密假设) $\{m\}_K = \{m'\}_{K'} \Leftrightarrow m = m' \wedge K = K'$。

## 3 802.11i 协议串空间模型

802.11i 协议中参与通讯的主体有 3 个：申请者(客户端)、认证者(无线接入点)和 RADIUS 服务器。这些主体都是网络设备的逻辑实体。

本文只讨论 802.11i 协议认证阶段的安全性。在这个阶段，申请者向认证者发送一个起始消息。认证者随后询问申请者的身份，申请者进行应答。认证者把应答转发给 RADIUS 服务器，RADIUS 服务器判断申请者是否是一个合法主体。为了进行判断，RADIUS 服务器发起一个挑战并把它发送给认证者。认证者把这个挑战转发给申请者。申请者对挑战进行应答，并通过认证者发送给 RADIUS 服务器，RADIUS 服务器做出接收或者拒绝的回应。成功的认证意味着申请者和认证者互相验证了对方的身份并生成用于随后数据传输的共享秘密。

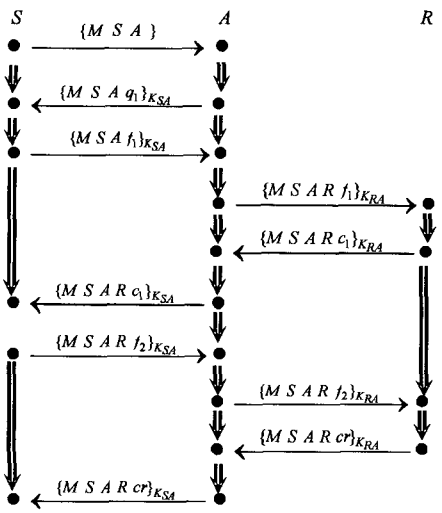


图 1 802.11i 协议的串空间

图 1 中，用串空间模型抽象描述了 802.11i 协议的认证过程。$S$，$A$ 和 $R$ 分别表示申请者、认证者和 RADIUS 服务器，$M$ 表示这些主体间交换的消息的集合。项 $\{MSARc_1\}_{K_{SA}}$ 表示用 $S$ 和 $A$ 的共享密钥加密的消息。认证者的询问集合表示为 $q=\{q_1,q_2,\cdots\}$，申请者应答集合 $f=\{f_1,f_2,\cdots\}$，RADIUS 服务器的挑战集合 $c=\{c_1,c_2,\cdots\}$，回应为 $c_r$。

申请者串用 $S_{sup}$ 表示，$S_{sup} \in \mathrm{Sup}[M,S,A,R,c_i,q_j,f_k,K_{SA}]$。根据图 1，迹可表示为 $\langle +\{MSA\}, -\{MSAq_1\}_{K_{SA}}, +\{MSAf_1\}_{K_{SA}}, -\{MSARc_1\}_{K_{SA}}, +\{MSARf_2\}_{K_{SA}}, -\{MSARc_r\}_{K_{SA}} \rangle$。类似地，认证者串 $S_{auth} \in \mathrm{Auth}[M,S,A,R,c_i,q_j,f_k,K_{SA},K_{RA}]$，迹为 $\langle -\{MSA\}, +\{MSAq_1\}_{K_{SA}}, -\{MSAf_1\}_{K_{SA}}, +\{MSAf_1\}_{K_{RA}}, -\{MSARc_1\}_{K_{RA}}, +\{MSARc_1\}_{K_{SA}}, -\{MSARf_2\}_{K_{SA}}, +\{MSARf_2\}_{K_{RA}}, -\{MSARc_r\}_{K_{RA}} \rangle$。RADIUS 服务器串 $S_{RADIUS} \in \mathrm{Radius}[M,S,A,R,f_k,c_i,K_{RA}]$，迹为 $\langle -\{MSAf_1\}_{K_{RA}}, +\{MSARc_1\}_{K_{RA}}, -\{MSARf_2\}_{K_{RA}}, +\{MSARc_r\}_{K_{RA}} \rangle$。

## 4 认证安全性分析

串空间模型中的认证是根据 Gavin Lowe 提出的一致(agreement)属性[6]来表述和验证的。协议保证参与者 $B$(响应者)就某个数据项 $X$ 达成一致。如果每次 $B$ 作为响应者使用数据 $X$ 与它所认为的 $A$(发起者)完成一轮协议执行时，确实存在惟一的一轮协议执行，其中 $A$ 作为发起者也使用 $X$，并且认为它的响应者为 $B$。

### 4.1 申请者的一致属性

申请者的一致属性可表述为下面的命题。

**命题 1** 设 $\Sigma$ 是 802.11i 协议的串空间，$C$ 是包含一个丛高为 6 的申请者串 $S_{sup} \in \mathrm{Sup}[M,S,A,R,c_i,q_j,f_k,K_{SA}]$ 的丛，$q_j$，$c_i$ 唯一生成于 $\Sigma$ 中，$K_{SA} \notin K_P$，$K_{RA} \notin K_P$，那么 $C$ 包含一个丛高为 10 的认证者串 $S_{auth} \in \mathrm{Auth}[M,S,A,R,c_i,q_j,f_k,K_{SA},K_{RA}]$ 和一个丛高为 4 的 RADIUS 服务器串 $S_{RADIUS} \in \mathrm{Radius}[M,S,A,R,f_k,c_i,K_{RA}]$。

证明：图 1 中申请者串 $S_{sup}$ 的迹为 $\langle +\{MSA\}, -\{MSAq_1\}_{K_{SA}}, +\{MSAf_1\}_{K_{SA}}, -\{MSARc_1\}_{K_{SA}}, +\{MSARf_2\}_{K_{SA}}, -\{MSARc_r\}_{K_{SA}} \rangle$。

下面首先说明项 $\{MSARc_r\}_{K_{SA}}$ 在丛 $C$ 中的一个正常结点生成。

对于 $\Sigma$ 中的一个丛 $C$，根据假设 $K_{SA} \notin K_P$，即入侵者不知道 $S$，$A$ 的共享密钥。下面考查入侵者的各种可能行为。

$M$：此时入侵者串的形式是 $\langle +t \rangle$。$M$ 串只有一个正结点，这意味着入侵者发送一个不是之前从其他结点得到的项。在这里，这个项是 $\{MSARc_r\}_{K_{SA}}$。由于 $K_{SA} \notin K_P$，入侵者不能生成一个用 $K_{SA}$ 加密的项，因此 $\Sigma$ 中不会有 $M$ 串。

$F$：此时入侵者串的形式是 $\langle -g \rangle$。因为生成结点总是正结点，所以 $\{MSARc_r\}_{K_{SA}}$ 不会在入侵者结点生成。

$T$：入侵者串的形式是 $\langle -g,+g,+g \rangle$。由于入侵者在第一个结点接收到项，这个项就不会是入侵者生成的，因此 $\{MSARc_r\}_{K_{SA}}$ 不会在 $T$ 串生成。

$C$：串的形式是 $\langle -g,-h,+gh \rangle$。入侵者接收到两个项，把它们级联形成一个新项并发送。由于通过简单的级联不会得到一个新项，因此 $\{MSARc_r\}_{K_{SA}}$ 不会在 $C$ 串生成。

$S$：串的形式是 $\langle -gh,+g,+h \rangle$。因为入侵者是从前面

(下转第 191 页)

置，这对于该算法的推广应用很有益处。基于典型测试函数的实验结果验证了新算法的正确性和高效性。

另外，FS算法的研究刚刚开始，进一步研究其生物学背景、深入挖掘该算法的潜力、充分发挥其寻优潜能，同时和其他进化算法构成混合算法，以及新算法在工程中的应用等方面都是值得研究的课题。

## 参 考 文 献


[1] Denbya B. Swarm intelligence in optimisation problems. Nuclear Instruments and Methods in Physics Research, 2003, 502: 364-368

[2] Elbeltagia E, Hegazyb T, Griersonb D. Comparison among five evolutionary-based optimization algorithms[J]. Advanced Engineering Informatics, 2005, 19: 43-53

[3] Rafal K, Tomasz A, Kenneth D J. Evolutionary computation and structural design: A survey of the state-of-the-art. Computers and Structures, 2005, 83: 1943-1978

[4] Dorigo M, Blum C. Ant colony optimization theory: A survey [J]. Theoretical Computer Science, 2005, 344: 243-278

[5] Kennedy J, Eberhart R. Particle swarm optimization [A]// Proc. IEEE Int. Conf. on Neural Networks [C]. Perth, WA, Australia, 1995: 1942-1948

[6] Penev K. Adaptive computing in support of traffic management [J]. Adaptive Computing in Design and Manufacturing, 2004: 295-306

[7] 周晖，等. 一种新的群集智能算法——自由搜索[J]. 东华大学学报：自然科学版，2007，33(5)：579-583

[8] 周晖，等. 一种新的群集智能优化及其改进研究[J]. 系统工程与电子技术，2008，30(2)：337-340

[9] Trelea I C. The particle swarm optimization algorithm: convergence analysis and parameter selection [J]. Information Processing Letters, 2003, 85(6): 317-325


(上接第 139 页)

的结点得到项 $g$ 和 $h$，$S$ 串没有正的生成结点。

$K$：这个串发送密钥〈$+K$〉。串空间模型中限定密钥不会和任何加密的消息相同，所以 $\{MSARc_r\}_{K_{SA}}$ 不会在入侵者的 $K$ 串生成。

$E$：串的形式是〈$-K, -h, +\{h\}_K$〉。在这里 $\{h\}_K = \{MSARc_r\}_{K_{SA}}$。根据自由加密假设，有 $h = \{MSARc_r\}$，$K = K_{SA}$。这意味着入侵者在第一个结点接收到密钥 $K_{SA}$。由于合法主体不会发送没有加密的秘密密钥，因此，$\{MSARc_r\}_{K_{SA}}$ 不会在 $E$ 串生成。

$D$：串的形式是〈$-K^{-1}, -\{h\}_K, +h$〉。由于为正的项是由接收到的消息解密得到的，没有正结点作为生成结点，因此，$\{MSARc_r\}_{K_{SA}}$ 不会在 $D$ 串生成。

由以上分析可知，$\{MSARc_r\}_{K_{SA}}$ 不会在入侵者结点生成，因此 $\{MSARc_r\}_{K_{SA}}$ 在丛 $C$ 中的一个正常结点生成。

同理，可以证明 $\{MSARc_r\}_{K_{RA}}$ 也在丛 C 中的一个正常结点生成。

结合图 1，生成 $\{MSARc_r\}_{K_{SA}}$ 的正常结点只能是申请者结点，生成 $\{MSARc_r\}_{K_{RA}}$ 的正常结点只能是 RADIUS 服务器结点。因为项 $\{MSARc_r\}_{K_{SA}}$ 出现在认证者串的最后一个结点，根据丛 $C$ 的属性，可知认证者串的丛高为 10。同样，$\{MSARc_r\}_{K_{RA}}$ 出现在 RADIUS 服务器串的最后一个结点，这使得 RADIUS 服务器串的丛高为 4。

### 4.2 认证者的一致属性

**命题 2** 设 $\Sigma$ 是 802.11$i$ 协议的串空间，$C$ 是包含一个丛高为 10 的认证者串 $S_{auth} \in \mathrm{Auth}[M, S, A, R, c_i, q_j, f_k, K_{SA}, K_{RA}]$ 的丛，$f_k, c_i$ 唯一生成于 $\Sigma$ 中，$K_{SA} \notin K_p$，$K_{RA} \notin K_p$，那么 $C$ 包含一个丛高至少为 5 的申请者串 $S_{sup} \in \mathrm{Sup}[M, S, A, R, c_i, q_j, f_k, K_{SA}]$ 和一个丛高为 4 的 RADIUS 服务器串 $S_{RADIUS} \in \mathrm{Radius}[M, S, A, R, f_k, c_i, K_{RA}]$。

证明：$S_{auth}$ 的迹是〈$-\{MSA\}, +\{MSAq_1\}_{K_{SA}}, -\{MSAf_1\}_{K_{SA}}, +\{MSAf_1\}_{K_{RA}}, -\{MSARc_1\}_{K_{RA}}, +\{MSARc_1\}_{K_{SA}}, -\{MSARf_2\}_{K_{SA}}, +\{MSARf_2\}_{K_{RA}}, -\{MSARc_r\}_{K_{RA}}$〉。

采用命题 1 的分析方法，可以推断出 $\{MSARc_r\}_{K_{RA}}$ 在丛 $C$ 中的一个正常结点生成，并且 $\{MSARc_r\}_{K_{RA}}$ 是在 RADIUS 服务器串的最后一个结点生成，从而 RADIUS 服务器串的丛高为 4。类似地，可以推断出项 $\{MSARf_2\}_{K_{SA}}$ 位于一个正常的申请者串上。从图 1 可以看出，$\{MSARf_2\}_{K_{SA}}$ 位于申请者串的第 5 个结点，因此申请者串的丛高是 5。这里不能保证申请者串的丛高为 6，因为存在入侵者丢弃合法主体消息的情况。

**结束语** 安全协议的形式化分析对于确保协议的正确性至关重要。本文利用串空间理论模型化了 IEEE802.11i 协议的认证过程。分析表明，802.11i 协议能够安全实现它的认证功能，并且分析过程简单直观。今后的工作包括在串空间模型中引入计算方法的观点[7,8]，使分析结果具有计算可靠性，以及形式化分析 802.11i 协议的其他安全属性。

## 参 考 文 献


[1] IEEE Std 802.11i™ Amendment 6: Medium Access Control (MAC) Security Enhancements[S], 2004

[2] Thayer F, Herzog J C, Guttman J D. Strand spaces: proving security protocols Correct [J]. Journal of Computer Security, 1999, 7(2): 191-230

[3] Yang Jie, Deng Huifang. Security electronic commerce protocol by the third kind entities[C]// 5th International Conference on Machine Learning and Cybernetics. IEEE Computer Society Press, 2006: 13-16

[4] 王继志，王英龙. 基于改进的串空间分析 Ad Hoc 路由协议安全性[J]. 软件学报，2006，17(11)：256-261

[5] Doghmi S F, Guttman J D, Thayer F. Sheletons, homomorphisms and shapes: characterizing protocol executions[J]. Notes Theor. Comput. Sci, 2007, 173: 85-102

[6] Lowe G. A hierarchy of Authentication Specifications[C]// 10th Computer Security Foundations Workshop Proceedings. IEEE Computer Society Press, 1997: 31-43

[7] Blanchet B. A computationally sound mechanized prove for security protocols[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 2006: 140-154

[8] Canetti R, Herzog J C. Universally composable symbolic analysis of mutual authentication and key exchange protocols[C]// 3th Theory of Cryptography Conference (TCC). Springer, 2006: 380-403