基于Q算法的认证协议漏洞挖掘技术研究*

吕乐乐，董　伟，赵云飞，冯　志，李致成，张雅勤
（华北计算机系统工程研究所，北京 102209）

摘　要： 认证授权协议在不泄露用户口令的情况下允许第三方获取用户资源，解决了云平台下第三方授权问题，提高了用户的交互体验。但是协议在交互处理中的不确定性和复杂性导致其在实际应用时可能会存在逻辑漏洞。针对该问题提出一种模糊仿真方法，通过对协议交互过程进行模糊处理，利用协议实体动作的不确定性，发现协议的逻辑漏洞。同时，结合SA-Q强化学习算法训练智能体学习最优模糊策略，智能化挖掘漏洞。经过测试发现，相比于基本的Q学习算法，该方法的收敛速度提升了9.27%，使得模型在训练时更容易收敛，有效提高了漏洞的挖掘效率。

关键词： 认证授权协议；逻辑漏洞；模糊仿真；Q强化学习算法
中图分类号： TN915.08　　**文献标识码：** A　　**DOI：**10.16157/j.issn.0258-7998.222641

中文引用格式： 吕乐乐，董伟，赵云飞，等. 基于Q算法的认证协议漏洞挖掘技术研究[J].电子技术应用，2022，48(10)：63-68.
英文引用格式： Lv Lele，Dong Wei，Zhao Yunfei，et al. Research on the vulnerability mining technology of authentication protocol based on Q-learning[J]. Application of Electronic Technique，2022，48(10)：63-68.

Research on the vulnerability mining technology of authentication protocol based on Q-learning

Lv Lele，Dong Wei，Zhao Yunfei，Feng Zhi，Li Zhicheng，Zhang Yaqin
（National Computer System Engineering Research Institute of China，Beijing 102209，China）

Abstract： The authentication and authorization protocol allows a third party to obtain user resources without disclosing the user password，solves the problem of third-party authorization under the cloud platform，and improves the user's interactive experience. However，the uncertainty and complexity of the protocol in interactive processing may lead to logical loopholes in its practical application. To solve this problem，a fuzzy simulation method is proposed. By fuzzy processing the protocol interaction process，the logical loopholes of the protocol are found by using the uncertainty of the action of the protocol entity. At the same time，combined with SA-Q reinforcement learning algorithm，the agent is trained to learn the optimal fuzzy strategy and mine the loopholes intelligently. After testing，it is found that compared with the basic Q-learning algorithm，the convergence speed of this method is improved by 9.27%，which makes the model easier to converge during training and effectively improves the efficiency of vulnerability mining.
Key words： authentication authorization protocols；logical vulnerabilities；fuzzy simulation；Q reinforcement learning algorithms

0 引言

随着互联网技术的不断发展，网络应用已经融入现实生活的方方面面。为了登录不同的网络应用，用户需要注册不同网站的账号信息[1]，并维护相应网站的账号和口令，低效而麻烦。认证授权协议允许第三方服务在无需用户提供账户和口令的情况下访问用户的私有资源，解决了当前开放云平台下的第三方授权问题，提高了用户的体验。但是当前网络环境复杂多样，且协议实体之间的交互存在着复杂的关系和制约，使得认证协议在交互处理中存在不确定性。因此，协议在实际使用时可能存在安全漏洞[2]，攻击者会利用协议本身的逻辑缺陷对信息系统进行攻击。

针对协议进行安全性分析是揭示协议缺陷和安全漏洞的重要方法。模糊测试是进行漏洞挖掘的常规方法[3]，其本质是变异报文字段取值，而非变异协议本身逻辑，因而只能发现协议编码实现的漏洞，不能发现协议逻辑上的漏洞。形式化方法是寻找协议逻辑缺陷的重要方法，其主要通过形式化分析工具对目标系统进行形式化建模[4]，但期间若存在较复杂的逻辑影响因素(如时延)，会使模型变得非常复杂，一方面可能会产生失真，另一方面可能会出现状态空间爆炸问题[5]。

为了避免“常规模糊测试查不了逻辑，形式化方法

* 基金项目：国家重点研发计划课题(2021YFB2012401)

模型复杂”的问题，本文提出一种新型方法-基于模糊仿真的漏洞挖掘方法，根据协议规约进行建模，基于Dolev-Yao模型[6]引入模糊体角色，以此制造交互过程中协议实体动作序列的不确定，结合SA-Q强化学习算法，协助模糊体进行动作选择与判断，挖掘协议逻辑漏洞。

1 相关工作

1.1 认证协议

认证协议是在通信过程中应用密码学技术隐藏或解密信息，达到身份认证以及消息正确发送的目的。在近年内许多提出的认证协议出现之初被认为是安全的[7]，但是在使用多年之后却被发现存在很严重的安全漏洞。

认证协议通常仅由几条消息组成，但是由于协议安全属性多样、逻辑结构复杂等特点，导致实际运用中存在诸多安全隐患，各种欺骗性和破坏性的攻击表明，其设计是一项高难度的工作[8]。若在逻辑上存在缺陷，执行过程中一个微小的安全漏洞就可能导致用户敏感数据暴露，使得攻击者在未授权的情况下访问系统，破坏网络服务的安全性。目前越来越多的认证协议正在涌现，关于其安全性性质的讨论方兴未艾。因此，在使用协议之前，对其进行安全性检测与分析至关重要。

1.2 Q学习算法

强化学习本质上是一种基于马尔科夫决策过程(Markov Decision Process)，训练智能体与环境交互，以实现智能体策略改进的机器学习算法[9]。其中典型算法Q学习利用三元组(S,A,R)来表征其智能体模型，如图1所示。

图1 Q学习算法结构图

强化学习的目的是寻找一个策略π，使得每个状态的值函数$Q^{\pi}(s)$达到最大。在决策过程中，智能体通过对当前状态的认知选择动作，环境接收该动作之后发生状态的转移[10]，智能体可以感知当前的状态s_t。交互环境会对该决策进行回应，给出相应的回报$R=R(s_t,a_t)$，之后进入下一个状态s_{t+1}[5]。状态值函数如式(1)所示：

$$Q_t(s_t,a_t)=Q_t(s_t,a_t)+\alpha(R_{t+1}+\gamma\max_a Q(s_{t+1},a)-Q(s_t,a_t)) \quad (1)$$

其中，α为学习率，$0\leqslant\alpha\leqslant1$。

2 模糊仿真模型构建

认证协议模糊仿真建模主要包括两部分：一是编码合法协议体交互过程和通信时的数据流；另一部分是构建模糊体，可通过选择模糊策略产生“混沌”交互的海量场景，利用SA-Q学习算法对协议状态分析，同时将智能体角色功能赋予给模糊体，通过维护Q表为下一步的行为提供建议，协助模糊体进行决策。模型框架图如图2所示。

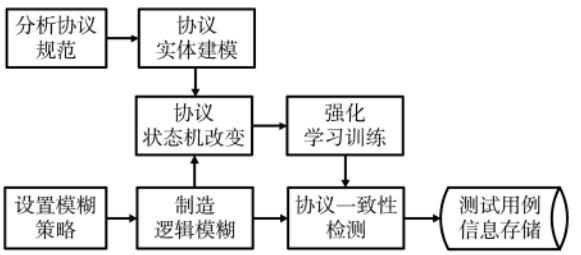

图2 模型架构图

针对认证协议自身的特点，设置以下前提条件：

(1)经过加密的消息只有知道正确的密钥才能对其进行解密；

(2)模糊体是参与协议交互的合法主体；

(3)模糊体熟知协议，有通信打包、解包、调用加解密算法的能力。

2.1 协议实体分析

首先根据协议RFC(Request For Comments)规约，分析参与协议的实体对象和报文参数，对目标协议的交互时序深入研究，构建协议交互模型，确认交互达到预期行为，搭建一个动态仿真环境代替真实运行环境。

在协议实体中参与者分为不同的角色，如图3所示。协议实体即遵守协议RFC规约参与协议交互的主体，包括诚实主体和模糊体。诚实主体是严格按照协议规范执行协议交互的主体，如认证用户、第三方网站、服务器等；模糊体是以破坏协议交互逻辑为目标的实体，其采用模糊策略扰乱交互顺序，期望在不被察觉的情况下获得诚实主体的信任，从而对协议的某个目标造成破坏。

2.2 模糊体构建

基于Dolev-Yao攻击者模型[6]的思想，引入模糊体角色。在协议交互过程中，模糊体采取主动攻击的思想，根据当前各状态机的状态选择模糊策略，协议交互环境将做出相应的改变。模糊策略包括：

(1)当前状态在转换处“选择点”时，可以选择非正常的状态迁移。测试过程从协议的第一次交互开始，测试时模糊体根据当前自身状态和环境状态，改变交互对象并且基于自己已有的知识库组合或重放报文。

(2)插入或者截获某段交互过程[11]。

(3)窃听其他交互消息。

在强化学习算法中，每一个动作可以视为一个攻击向量，用<target,operation>表示，其中target表示交互的对象，operation表示采取的模糊策略。环境的状态空间使用四元组(inter_phase,dat,own_state,env_state)表示，其中inter_phase表示运行到协议交互第几阶段，data表示

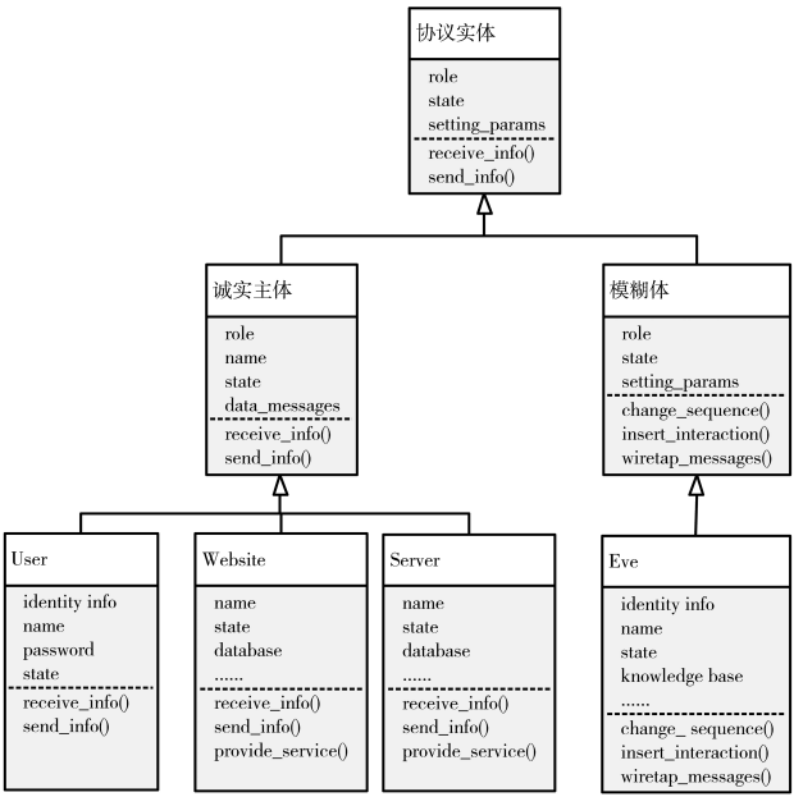

图 3 模糊仿真系统类图

接收的数据，own_state 表示交互之后协议主体自身的状态，env_state 表示当前环境状态或者其他主体状态。

认证协议最终需要按照协议规约，通过多次交互，达到参与者之间的单向认证或者双向认证。因此若违背认证协议的安全属性[12]，则表明协议存在逻辑漏洞：

(1)如果最后模糊体以其他合法实体的身份认证成功，却不符合协议规约的认证关系；

(2)模糊体获得其他用户的保密信息、关键参数等情况。

2.3 SA-Q 学习算法决策

为了引导测试走向深入，提高测试效率，采用 SA-Q 算法优化模糊体的决策行为。将认证协议漏洞挖掘的过程建模为马尔科夫决策模型，基于强化学习算法利用交互环境获取奖赏，训练模糊体选择最佳响应动作。

在训练过程中，模糊体初始回合对状态动作的经验了解较少，Q 学习算法基于贪婪策略容易导致局部最优[13]。SA-Q 学习算法将模拟退火算法的 Metropolis 准则[14]应用到动作搜索过程中，以解决局部最优的问题。当智能体选择动作时，除了迄今为止学习到的策略，也尝试选择当前最优策略以外的动作来探索，动作选择的概率表示为：

$$P(a|s)=e^{\frac{Q(s,a_t)-Q(s,a_g)}{\text{Temperature}}} \tag{2}$$

其中，$Q(s,a_t)$是随机选择动作的 Q 值；$Q(s,a_g)$是基于 ε-greedy 策略选择动作的 Q 值；Temperature 为退火温度值，按照几何比例因子准则递减。初始回合训练时，Temperature 值较大，模糊体探索的随机性概率较高；后续随着温度下降，基于 ε-greedy 策略选择动作逐渐占据主导策略，以达到动作探索和利用的平衡[14]。

算法中回报函数反映了当前状态下执行不同动作的效果，发现漏洞的效率很大程度取决于对执行动作的评价。本文动作评价标准如下：如果模糊体通过动作选择之后达到下一个状态节点，没有按照协议规约的动作序列且交互环境产生新的状态，根据模糊体当前处于的交互阶段给予奖励，公式如下：

$$\text{temp}=\begin{cases}1 & \text{满足条件}\\ -1 & \text{不满足条件}\end{cases} \tag{3}$$

$$r=\text{temp}\times 100\times \text{phase(fuzzy body)}\times \text{Scale factor} \tag{4}$$

其中，phase(fuzzy body)代表模糊体利用模糊策略进行到协议交互的第几个阶段，如果交互阶段越偏后，说明模糊体越有可能攻击成功，因此回报值的大小与协议交互的阶段成比例；Scale factor 代表折扣因子，取值为 0.6。实验采用回合制的方式进行，在每次回合中，通过一次次的动作选择，与外界环境交互得到反馈结果，计算回报函数，不断优化更新 Q 表从而实现策略改进。

3 实验仿真与结果分析

3.1 实验过程

Needham-Schroeder 协议(NSPK 协议)是一个经典的安全协议，一直被优先选为新的协议分析方法的测试对象。协议最终的目的是通信双方完成双向的身份认证。本节以 NSPK 协议为例进行测试，分别基于 Q 学习算法、SA-Q 算法建模，在相同交互环境下测试实验效果。

本文方法的流程图如图 4 所示。

模糊仿真协议建模的第一步是构建协议交互实体，参数设置如表 1 所示。

其中，Alice、Bob、Eve 是协议本身的合法主体，除此之外 Eve 为模糊体。Eve 基于 SA-Q 学习算法的决策方法根据当前协议体状态选择动作，充当一个有经验考虑长久化利益的交互体，以期待从交互中获得长期积累奖励的最大值。若交互中检测到协议体产生新的状态，则给予奖赏。算法中设置学习率 α=0.01，贪心策略 ε=0.9，折扣因子 γ=0.8，降温等比系数为 0.6，温度 Temperature 取值 350，增加模糊体选择随机动作的概率。

3.2 实验结果

从初始状态开始，协议交互的部分路径简化如下所示，其中 Eve( )代表 Eve 没有伪装其他主体的情况，仅接收或发送消息；Eve(user)代表 Eve 冒充 user 身份进行

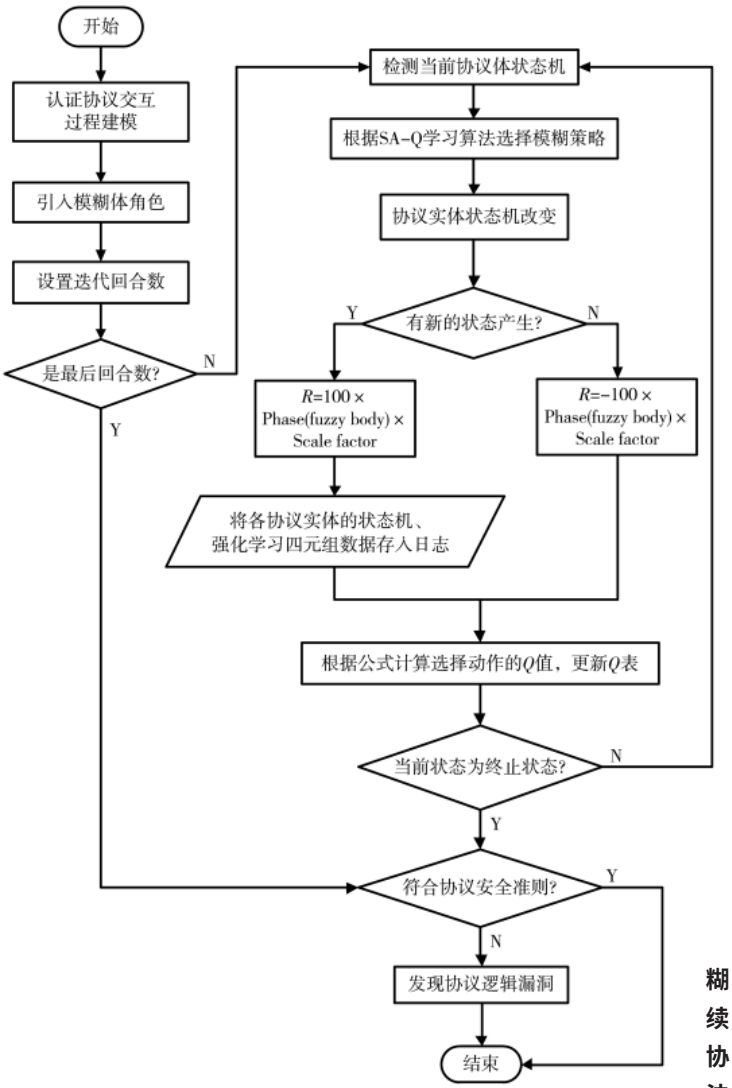

图 4 模型流程示意图

表 1 协议参数

参数	样例	备注
协议实体	Alice Bob Eve	参与协议交互的主体
新鲜值	N_A N_B	表示协议实体 Alice、Bob 在协议运行时生成的随机数值
身份信息	Ainfo Binfo	表示协议实体 Alice、Bob 的身份信息
密钥集合	PK_Bob PK_Alice PK_Eve ……	包括各实体的公钥、私钥

交互、重放或者修改交互数据。

路径 1：

Alice→Eve( )：$\{Ainfo, N_A\}_{PK\_Eve}$

Eve( )→Alice：$\{N_A, N_i\}_{PK\_Alice}$

Alice→Eve( )：$\{N_i\}_{PK\_Eve}$

Note：Attack fail

路径 2：

Alice→Eve(Bob)：$\{Ainfo, N_A\}_{PK\_Bob}$

Eve(Alice)→Bob：$\{Ainfo, N_A\}_{PK\_Bob}$

Bob→Eve(Alice)：$\{N_A, N_B\}_{PK\_Alice}$

Eve( )→Bob：$\{\{N_A, N_B\}_{PK\_Alice}\}_{PK\_Bob}$

Note：Attack fail

路径 3：

Alice→Eve(Bob)：$\{Ainfo, N_A\}_{PK\_Bob}$

Eve(Alice)→Bob：$\{Ainfo, N_A\}_{PK\_Bob}$

Bob→Eve(Alice)：$\{N_A, N_B\}_{PK\_Alice}$

Eve(Bob)→Alice：$\{N_A, N_B\}_{PK\_Alice}$

Alice→Eve(Bob)：$\{N_B\}_{PK\_Bob}$

Eve(Alice)→Bob：$\{N_B\}_{PK\_Bob}$

Note：Attack fail

路径 4：

……

路径 n：

Alice→Eve( )：$\{Ainfo, N_A\}_{PK\_Eve}$

Eve(Alice)→Bob：$\{Ainfo, N_A\}_{PK\_Bob}$

Bob→Eve(Alice)：$\{N_A, N_B\}_{PK\_Alice}$

Eve( )→Alcie：$\{N_A, N_B\}_{PK\_Alice}$

Alice→Eve( )：$\{N_B\}_{PK\_Eve}$

Eve(Alice)→Bob：$\{N_B\}_{PK\_Bob}$

Note：Attack succeed

实验结果表明初始训练时，由于 Q 表尚未完善，模糊体学习轨迹偏向于随机化，会呈现多种交互情况；后续随着 Q 表迭代更新，学习效率逐渐提高，表明易于在协议混乱交互环境下发现攻击路径。上述路径 4 表明算法发现了该协议的逻辑漏洞，NSPK 协议测试中，模糊体 Eve 通过伪装协议体 Alice，维护 Alice 的状态机和合法身份的状态机，完成了与 Bob 的身份认证，是典型攻击中的穿插攻击，并且最终发现的攻击路径和形式化软件 Scyther[15] 发现的攻击路径相同，其攻击轨迹如下所示：

协议会话 1 消息 1：Alice→Eve：$\{Ainfo, N_A\}_{PK\_Eve}$

协议会话 2 消息 1：Eve(Alice)→Bob：$\{Ainfo, N_A\}_{PK\_Bob}$

协议会话 2 消息 2：Bob→Eve(Alice)：$\{N_A, N_B\}_{PK\_Alice}$

协议会话 1 消息 2：Eve→Alice：$\{N_A, N_B\}_{PK\_Alice}$

协议会话 1 消息 3：Alice→Eve：$\{N_B\}_{PK\_Eve}$

协议会话 2 消息 3：Eve(Alice)→Bob：$\{N_B\}_{PK\_Bob}$

3.3 模型仿真分析

3.3.1 算法性能

基于控制变量的方法，在实验场景下使用同样的一组超参数测试 Q 学习算法、SA-Q 学习算法的性能，选择平均奖励值作为评价指标，算法在一定交互次数之后得到的平均奖励值数据对比如表 2 所示，数据变化趋势如图 5 所示。

图 5 中，SA-Q 的奖励值在训练初始阶段小于 Q 学

表 2 算法改进前后训练结果对比

算法	平均奖励值	训练步长
Q	100.22	151
SA-Q	120.19	137

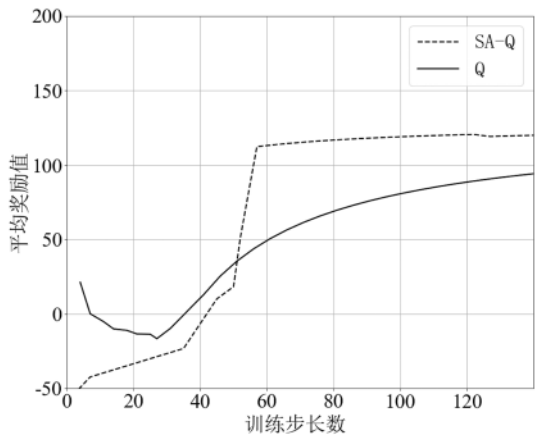

图 5 算法改进前后不同训练步长下的平均奖励值

习算法的奖励值，随着训练回合数增加，模糊体对环境知识的认知提高，大约在 137 步之后奖励值趋于收敛。基本 Q 学习算法在大约 150 步学习之后性能仍次于前者，并且奖励值还未达到收敛状态。因此可以得出结论：(1)基于 SA-Q 探索算法在一段时间学习之后其动作策略优于 Q 学习算法的策略；(2)SA-Q 学习算法的收敛速度更快，奖励值更快趋于稳定。

一次训练回合结束后，如果模糊体发现攻击路径代表一次胜利[16]。胜利概率是训练过程中胜利次数的总和与总的回合数 episode 的比值，模糊体在不同回合下的胜利概率如图 6 所示。

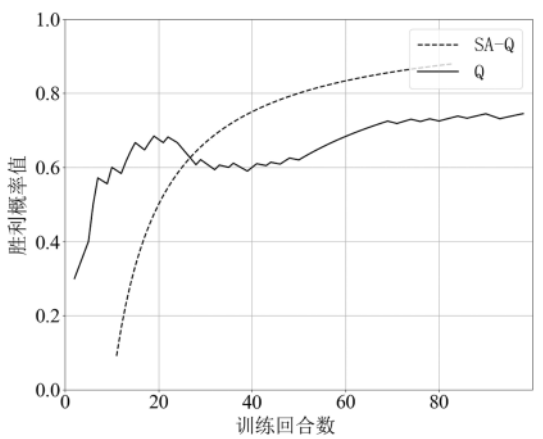

图 6 算法改进前后的胜利概率

从图 6 中可以看出，在训练初始阶段，Q 学习算法的胜利概率相对较高；但后续 SA-Q 学习算法在接近 30 回合时超过 Q 学习算法的胜利概率，并且随着训练回合数的增加，胜率概率逐渐趋于 1。

3.3.2 漏洞探测能力

基于 SA-Q 学习模糊仿真模型参照协议 RFC 规约和交互报文，清晰直观地描述协议实体交互过程和相应的状态机，实现了协议全范围的模拟仿真。

该模型发现了 NSPK 协议的逻辑漏洞，从攻击过程可知 NSPK 协议的安全性依赖于不同参与者的合法身份标识，侧面反映认证中心和协议体之间的密钥加密并不是完全可靠的。通过设置模糊策略，呈现出协议深入交互的多场景，实现协议多角色身份交互的动态测试，有助于发掘更深层次的新型协议漏洞。

4 结论

本文针对传统测试技术缺乏对认证协议逻辑漏洞挖掘的问题，提出了一种基于 SA-Q 学习算法的模糊仿真测试方法，以 Needham-Schroeder 公钥协议为例，确定协议参与者和协议认证的安全属性，结合 Dolev-Yao 模型引入模糊体角色，在拥有合法身份的前提下进行逻辑模糊，检测出协议的穿插攻击，证实了建模的准确性和有效性。

模糊仿真思想考虑了协议多会话交互、多方参与的特殊场景，在模拟系统各部分的协议交互中，增设有关机制模糊化处理，对协议交互逻辑进行深入分析。本文将 SA-Q 学习算法与 Q 学习算法进行对比分析，初步结果表明，SA-Q 学习算法在收敛速度方面优于标准 Q 学习算法。当前基于强化学习的漏洞挖掘仍处于模拟验证阶段，但使用虚拟化手段在仿真环境训练智能体是未来的研究方向，在后续的工作中，针对复杂交互的认证协议，需要进一步完善模型和模糊策略，考虑使用基于神经网络的强化学习算法来调整模糊规则库和状态动作空间，使之具有泛化能力，增强模型的扩展性。

参考文献

[1] 刘奇旭，邱凯丽，王乙文，等.面向 OAuth2.0 授权服务 API 的账号劫持攻击威胁检测[J].通信学报，2019，40(6)：40-50.

[2] 杨锦翔，熊焰，黄文超.基于强化学习的安全协议形式化验证优化研究[J].计算机工程，2021，47(12)：141-146.

[3] FENG X，SUN R，ZHU X，et al.Snipuzz：black-box fuzzing of IoT firmware via message snippet inference[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security，2021：337-350.

[4] 陆思奇，周思渊，毛颖.强安全模型下 TLS1.3 协议的形式化分析与优化[J].软件学报，2021，32(9)：18.

[5] AIRESURQUIZA A，ALTURKI M，BANKIRIGIN T，et al.Resource and timing aspects of security protocols[J].Journal of Computer Security，2021，29(2)：1-42.

[6] SABINA S.Security protocols analysis including various time parameters[J].Mathematical Biosciences and Engineering，2021，18(2)：1136-1153.

[7] 张正，查达仁，柳亚男，等.基于物理不可克隆函数的

Kerberos 扩展协议及其形式化分析[J].信息网络安全，2020，20(12)：91-97.
[8] SINISA T，MILICA K，MIHALJEVIC M J.Analysis and correction of the attack against the LPN-problem based authentication protocols[J].Mathematics，2021，9(5)：573-574.
[9] KOSTRIKOV I，NAIR A，LEVINE S.Offline reinforcement learning with implicit Q-learning[J].arXiv preprintarXiv：2110.06169，2021.
[10] 张书钦，李凯江，张露，等.基于Q-learning机制的攻击图生成技术研究[J].电子科技，2018，31(10)：6-10.
[11] 龚翔，冯涛，杜谨泽.基于CPN的安全协议形式化建模及安全分析方法[J].通信学报，2021，42(9)：240-253.
[12] 顾纯祥，王焕孝，郑永辉，等.基于SAT的安全协议惰性形式化分析方法[J].通信学报，2014，35(11)：117-125.
[13] ZHUANG H，DONG K，QI Y，et al.Multi-destination path planning method research of mobile robots based on goal of passing through the fewest obstacles[J].Applied Sciences，2021，11(16)：7378.
[14] ROVIRA-SUGRANES A，AFGHAH F，QU J，et al.Fully-echoed Q-routing with simulated annealing inference for flying adhoc networks[J].IEEE Transactions on Network Science and Engineering，2021，8(3)：2223-2234.
[15] CABUK U C，DALKILIC G，DAGDEVIREN O.CoMAD：context-aware mutual authentication protocol for drone networks[J].IEEE Access，2021，9：78400-78414.
[16] Lin Guichao，Zhu Lixue，Li Jinhui，et al.Collision-free path planning for a guava-harvesting robot based on recurrent deep reinforcement learning[J].Computers and Electronics in Agriculture，2021，188：106350.

(收稿日期：2022-02-14)

作者简介：
吕乐乐(1997-)，女，硕士研究生，主要研究方向：漏洞挖掘、强化学习。
董伟(1986-)，通信作者，男，硕士，高级工程师，主要研究方向：计算机网络安全、渗透测试、工控信息安全检测，E-mail：keepersecuritys@163.com。
赵云飞(1969-)，男，硕士，教授级高工，主要研究方向：强化学习、工业控制系统信息安全、计算机网络安全。

扫码下载电子文档

(上接第62页)

量，减小对远端基站的干扰强度，通过对本端小区远程电调来实现对小区覆盖范围的收缩，降低对远端小区的干扰，实现对干扰源强度的抑制。

4 结论

5G发展是当前主流趋势，无线通信无法避免受到外部干扰，大面积5G站点建设需要关注远端干扰带来的负面影响，根据5G系统及大气波导干扰特点，仍可借鉴TD-LTE大气波导应对经验制定相应的定位、规避措施。同时，5G TDD系统在实际部署场景中可以使用新技术来有效规避远端干扰，如修改特殊子帧GP长度、调整时隙配比避开强干扰区域、优化超高站点等。

参考文献

[1] 李常国，李国强，贺庆.2.6GHz频段5G大气波导干扰研究[J].山东通信技术，2019，39(4)：14-16.
[2] 许国平.大气波导干扰对5G NR的影响预研和应对措施探讨[J].邮电设计技术，2019，9(8)：34-39.
[3] 仇勇，郑英，魏志刚，等.TDD系统大气波导干扰研究与应对[J].电信工程技术与标准化，2018，31(9)：40-45.
[4] 唐志波.大气波导对LTE系统的干扰及预防策略[J].信息通信，2018，12(10)：207-208.
[5] 赵洪锋，王超，秘俊杰.TD-LTE网络大气波导干扰研究[J].电信工程技术与标准化，2017，30(9)：73-78.
[6] 张力伟，梁纪兴，秘俊杰.大气波导干扰及解决方案[J].电信工程技术与标准化，2017，30(10)：35-39.
[7] 吕芳迪，郭宝.TD-LTE干扰优化中对大气波导的监测与规避[J].电信工程技术与标准化，2016，29(11)：1134-1139.
[8] 周朋，张海勇，贺寅，等.大气波导在海上通信中的应用[J].电讯技术，2014，15(8)：84-88.

(收稿日期：2021-07-14)

作者简介：
金淼(1972-)，男，本科，工程师，主要研究方向：无线通信网络的规划、设计、优化等。
樊忠文(1992-)，男，硕士，工程师，主要研究方向：无线通信网络规划、优化等。

扫码下载电子文档

版权声明