计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(12):398−404 [doi: 10.15888/j.cnki.csa.008956]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

5G 网络认证与密钥协商协议的形式化验证与分析①

杨成龙, 杨晋吉, 苏桂钿, 管金平

(华南师范大学 计算机学院, 广州 510631)
通信作者: 杨晋吉, E-mail: yangjj@scnu.edu.cn

摘　要: 网络攻击的手段层出不穷, 如中间人攻击, 重放攻击, DoS 攻击等, 以此获取不当利益. 密钥协商协议的设立是为合法用户提供正确认证入口, 并拒绝攻击者的非法接入和攻击. 密钥协商协议是保护移动通信提高服务质量的第一道安全防线, 5G 网络密钥协商协议在实际环境中仍然存在安全隐患, 其协议本身的安全特性能否满足要求仍未可知, 本文提出使用基于概率模型检测的方法, 通过对 5G 网络密钥协商协议的各协议方实体进行建模, 建立离散时间马尔科夫链模型, 在建模过程中考虑外界的攻击影响, 引入攻击率来描述外界的影响程度, 通过攻击率对 5G 网络密钥协商协议的研究进行定量分析, 使用概率计算树逻辑对待验属性规约进行编码描述, 利用概率模型检测工具 PRISM 进行实验. 实验结果表明: 在引入攻击率的 5G 网络密钥协商协议模型中, 5G 网络密钥协商协议各协议方实体所受攻击的影响对该协议的时延性, 有效性, 保密性等属性规约的性能有不同程度的影响, 因此, 研究外界网络攻击对协议的安全性能的影响, 对加强协议安全性能及其改进具有一定借鉴意义, 并对 5G 网络密钥协商协议的安全特性的提升和保护用户的经济与信息安全具有很大的意义.

关键词: 概率模型检测; 5G 网络; 认证与密钥协商协议; 形式化验证; PRISM

引用格式: 杨成龙,杨晋吉,苏桂钿,管金平.5G 网络认证与密钥协商协议的形式化验证与分析.计算机系统应用,2022,31(12):398–404. http://www.c-s-a.org.cn/1003-3254/8956.html

Formal Verification and Analysis of Authentication and Key Agreement for 5G Networks

YANG Cheng-Long, YANG Jin-Ji, SU Gui-Tian, GUAN Jin-Ping

(School of Computer Science, South China Normal University, Guangzhou 510631, China)

Abstract: There are numerous methods of network attacks, such as man-in-the-middle attacks, replay attacks, and DoS attacks, which are ways to gain improper benefits. The authentication and key agreement (AKA) is set up to provide a correct authentication portal for legitimate users and deny illegal access and attacks from attackers. AKA is the first line of security to protect mobile communications for higher quality of service. The AKA for 5G networks still has security problems in the actual environment, and it is still unknown whether the security features of AKA can meet the requirements. Therefore, this study proposes to use the method based on probabilistic model checking to build a discrete-time Markov chain model by modeling each protocol party entity of AKA for 5G networks. In the modeling process, the influence of external attacks is considered, and the attack rate is introduced to describe the degree of external influence. The studies of AKA for 5G networks are quantitatively analyzed through the attack rate, and the probabilistic computation tree logic is employed to describe the codes of the specifications for the a priori attributes. Experiments are conducted by the probabilistic model checking tool PRISM. The experimental results indicate that in the AKA model with the introduction of the attack rate, the attacks on each protocol party entity of AKA for 5G networks have different influences

① 基金项目: 广东省自然科学基金 (2020A1515010445)
收稿时间: 2022-06-03; 修改时间: 2022-08-19; 采用时间: 2022-08-25; csa 在线出版时间: 2022-10-28

on the performance of the attribute specifications such as delay, validity, and confidentiality of the protocol. Therefore, the study of the impact of external network attacks on the security performance of the protocol has certain implications for strengthening the security performance of the protocol and its improvement, and it is of great significance to enhance the security features of AKA for 5G networks and protect the economic and information security of users.

Key words: probabilistic model checking; 5G networks; authentication and key agreement (AKA); formal verification; PRISM

1 引言

随着网络移动通信的发展, 对通信协议的要求越来越高. 时延低, 速率高是 5G 网络通信新的业务特点, 移动通信技术的变革往往会带着巨大的潜在的安全隐患, 5G 技术引入带来新风险, 依靠传统物理隔离的体系不再适用[1], 网络安全问题是行业必须关注和完善的问题之一. 认证协议是保护移动通信网络安全的第一道防线[2], 随着协议的优化, 不断地将参数, 网络和接入场景等纳入考虑范围[3], 对于认证协议安全特性的研究同样也是业界关注的重要领域.

移动通信系统的无线接口由于无线连接的特性向来是最容易遭受攻击的[4], 外界的各种不确定因素使得用户接入网络的安全性面临巨大的风险, 认证与密钥协商协议 (authentication and key agreement, AKA) 是移动通信重要认证协议之一, 非形式化的验证方法不能满足定量分析的要求, 且因该协议的复杂程度, 利用非形式化验证方法难以完成有效验证. 形式化方法是基于严格数学基础, 完备地证明或验证系统软件是否满足系统的需求规范. 本文针对 5GAKA 协议采用形式化验证方法研究在引入攻击率后, 研究协议的安全特性的影响, 本文结构首先对 5GAKA 协议及国内外研究现状进行简述, 其次介绍概率模型检测, 其次通过计算树逻辑描述待测性质进行实验, 最后通过实验分析得出实验结论, 利用实验结果, 在可控的范围内对协议进行控制或改进, 增加协议安全性和稳定性. 实验结果表明, 5GAKA 协议在一定程度的外界攻击下, 该协议的时延性、有效性、保密性都存在缺陷, 5GAKA 协议的研究对提升协议安全性能和改进具有一定借鉴意义.

2 5G 网络 AKA 协议及其现状

认证协议作为移动网络安全的第一层保护, 身份认证是安全领域研究一直是业界关注的重要方面[5]. 目前, 国内外学者已对 AKA 协议进行了相关的研究, 文献 [6] 针对 3G 鉴权认证协议的研究中发现存在 Linkability 攻击和 IMSI Paging 攻击, 并针对此攻击提出了修复方案. 文献 [7] 发现了一种针对 AKA 协议所有变体的新隐私攻击, 通过对这个逻辑漏洞的攻击可以获取用户隐私信息, 作者对漏洞进行安全分析, 提出了补救的对策. 文献 [8] 针对第 4 代移动电话, 特别是 4G LTE (long term evolution, LTE) 的隐私相关安全属性. 作者提出了一个攻击模型, 它使追踪受害者的移动设备成为可能, 最后提出了一个修改的认证协议. 文献 [9] 利用 ProVerif 和 NuSMV 工具分析了 4GLTE 协议, 提出了一种基于模型的测试方法 LTEInspector, 检测协议的潜在设计缺陷. 文献 [10] 利用安全协议验证工具 Tamarin 分析 5GAKA 协议. 文献 [11] 讨论了 5GAKA 协议的可链接性问题, 且证明 5GAKA 协议是 σ 不可连接的, 它允许对协议隐私进行细粒度量化, 最后改进了 5GAKA 协议的可链接性问题. 文献 [12] 使用 Tamarin 验证工具对 5GAKA 鉴权认证协议进行安全分析, 对出现的问题提出安全加固的方案以及对方案进行验证分析. 文献 [13] 梳理了 4G 和 5G 蜂窝网络的认证和隐私保护的方案, 并较为全面地对网络的威胁模型和应对策略进行了分类和总结, 并对应对策略进行了比较, 进一步给出了一些建议.

与 4GLTE 网络结构类似, 5G 移动通信网络也有 3 个协议实体, 分别为用户终端设备 (user equipment, UE), 服务域网络 (serving networks, SN) 以及归属域网络 (home networks, HN). 用户设备即终端设备, 包含用户永久标识, 协商公钥等数据. 服务域网络 SN 是终端设备可以接入网络, 终端设备与服务域网络是无线通信, 归属域网络 HN 是密钥协商协议的核心部分, 归属域网络 HN 和服务域网络 SN 是 5G 网络的核心网, 终端设备的身份验证通过核心网来验证, 而归属域网络与服务域网络 SN 是有线通信. 由于网络攻击的方式多种多样, 例如中间人攻击, 重放攻击, DoS攻击等, 在实

际环境下, 数据信息在交换传输的过程中会遭受恶意实体的攻击, 导致接收信息不完整或者丢失[14], 本文从 AKA 协议认证的过程研究受到攻击的后协议的安全性和稳定性. 本文主要工作是验证 UE 与 SN, 以及 SN 与 HN 交互信息传递过程的攻击对 AKA 协议的时延性, 有效性, 保密性能否满足系统需求, 量化属性的满足程度并对实验结果进行分析, 以提高协议安全性和服务质量.

3 概率模型检测概述

概率模型检测 (probability model checking)[15] 是形式化验证方法的一种自动验证技术[16], 通过穷举目标模型状态空间, 验证模型是否满足属性, 建立的目标模型是一种有限状态自动机, 状态空间包含系统可能达到的所有状态. 概率模型检测一般的步骤, 首先对待检测的系统建立模型, 根据系统的特点可以建立模型, 即描述系统的状态及行为. 而模型则包括离散时间马尔科夫链 (discrete-time Markov chains, DTMCs) 模型, 连续时间马尔科夫链 (continuous-time Markov chains, CTMCs) 模型, 马尔科夫决策过程 (Markov decision processes, MDPs), 实时模型 (probabilistic timed automata, PTAs), 部分可观察的概率时间自动机模型 (partially observable probabilistic timed automata, POPTAs) 和部分可观察的马尔科夫决策过程 (partially observable Markov decision processes, POMDPs) 等模型. 系统建模完成之后, 对待验证的属性通过时态逻辑进行描述, 时态逻辑有以下几种: 概率计算树逻辑 (probabilistic computation tree logic, PCTL), 连续随机逻辑 (continuous stochastic logic, CSL), 线性时序逻辑 (linear time logic, LTL) 以及同时包含 PCTL 和 LTL 的 PCTL*逻辑. 最后通过已建立的模型对待验属性进行定量分析. 本文采用离散时间马尔科夫链[17] 模型描述 5GAKA 协议的状态和行为, 使用概率计算树逻辑 PCTL 描述 5GAKA 协议的时延性、有效性、保密性 3 个待验证的属性规约. 最后根据试验结果对验证的属性进行分析.

3.1 离散时间马尔科夫链

根据研究的 5GAKA 协议特点, 采用离散时间马尔科夫链模型建模.

定义 1. 离散时间马尔科夫链是一个五元组.

$$M =< S, P, s_0, AP, L >$$

其中, S为一个有限非空状态集, $P = S \times S \to [0,1]$, 是概率转移函数, s_0是初始状态, AP是有限原子命题集, $L: S \to 2^{AP}$, 是原子命题的标签函数.

图 1 为离散时间马尔科夫链示例图, 有限非空状态集$S = \{s_0, s_1, s_2, s_3, s_4\}$, P为概率转移函数, s_0是初始状态, $L\{s_4\} = \{\text{end}\}$结束状态标志.

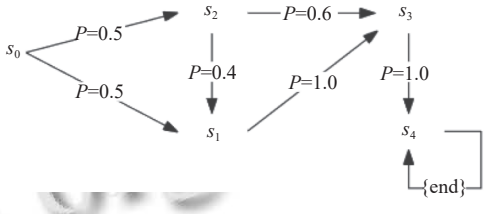

图 1 离散时间马尔科夫链实例

4 5GAKA 协议的验证

4.1 5GAKA 协议建模

用户设备 UE 协议实体在接入 5G 网络之前需要完成接入网络的身份验证, AKA 协议是确保在用户设备实体 UE, 服务域网络实体 SN 及归属域网络实体 HN 之间能够相互认证通信, 并保证在 UE 和 SN 之间建立一个安全的交互通道. 本节首先描述 AKA 协议各个协议实体在进行身份验证中相互认证的过程, 然后根据该协议交互的过程创建离散时间马尔科夫链模型并进行验证.

AKA 协议有 3 个协议实体分别为: 用户终端设备 UE, 服务域网络 SN, 归属域网络 HN. 通过对协议实体和交互过程建立离散时间马尔科夫链 (DTMC) 模型来描述该系统的行为和状态来验证协议的安全属性: 时延性 (time ductility)、 有效性 (effective)、 保密性 (confidential). AKA 协议交互过程复杂且本文就安全性质进行定量研究和分析, 因此就 AKA 协议交互过程进行大致描述. 第 1 阶段在 UE 进行接入网络之前, UE 实体需要进行身份的验证, UE 首先发送入网请求给 SN, SN 接收到 UE 的接入网络的请求并要求 UE 提供身份信息, UE 接收到 SN 的响应, 验证响应是否有效并发送 UE 的身份信息, 第 2 阶段 SN 接收到 UE 的身份信息并将身份信息发送给 HN 进行身份验证, HN 接收到 SN 发送信息, 验证 UE 的身份信息, 并给 SN 发送质询消息. 第 3 阶段 SN 接收到 HN 返回的质询消息, 将质询消息发送给 UE, UE 接收到质询消息,

首先验证其有效性, 若有效, 则将响应发送给 SN. 第 4 阶段 SN 接收到 UE 的响应, 将响应发送给 HN, HN 对响应进行认证, 若符合, 则表示用户鉴权认证成功, 可以接入网络. 然后将验证结果返回给 SN, 并在 SN 与 UE 之间建立一条通信线路, 此后的 UE 与 SN 的信息交互都是通过这条通信线路进行. 图 2 为 AKA 鉴权认证协议交互大致过程的流程图.

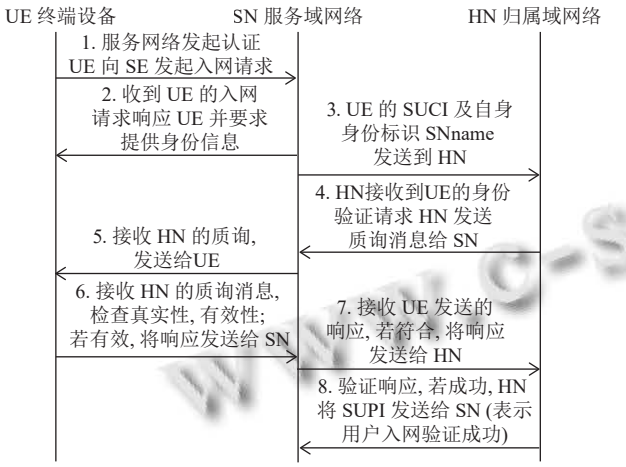

图 2 AKA 鉴权认证协议流程图

为了准确验证协议的性质, 本文采用模型检测工具 PRISM[18] 模型检测器对 AKA 协议建立离散型马尔科夫模型, 下面对建立的模型进行说明. 该模型有 3 个模块分别为: UE 模块, SN 模块, HN 模块. 每个模块都有多个用来描述模型的行为和状态的变量, UE 模块符号说明如表 1 所示.

本文将 AKA 协议划分为 4 个阶段进行. 每个模块进行交互的信息首先需要进行验证消息是否被截取, 即是否完整, 再进行下一步. 首先第 1 阶段, UE 向 SN 发送入网请求消息 1, SN 接收到 UE 的请求消息 1 先验证其消息的是否被攻击截取, 即验证消息 1 是否完整, 若不完整则模块 SN 异常结束, 若完整则 SN 发送响应消息 2 给 UE, UE 接收 SN 的响应消息 2, 验证消息 2 的完整性. 部分伪代码如下所示.

```
if Message1 没有发送
do 发送 Message1
if SN 未结束 and 满足条件 1 and Message2 未发送 and Message1 已发送
do 发送 Message2
if SN 未结束 and 满足条件 1 and Message2 未发送 and Message2 被攻击
do SN 结束
```

表 1 UE 模块符号说明

变量	范围	含义
FinishUE	True/False	False表示UE模块正常运行, True表示UE模块结束
SendMessage1	True/False	第1阶段是否向UE发送请求
SendMessage6	True/False	第3阶段是否向SN发送请求
CheckMessage2	[0, 2]	0表示没有验证响应消息, 1消息未被攻击, 2消息被攻击
CheckMessage5	[0, 2]	0表示没有验证响应消息, 1消息未被攻击, 2消息被攻击
attackES	[0, 1]	浮点型变量, 表示UE与SN之间通信被攻击的概率
attackNH	[0, 1]	浮点型变量, 表示SN与HN之间通信被攻击的概率
flag1	True/False	False第1阶段异常结束, True第1阶段正常结束

第 2 阶段 SN 接收到 UE 的身份信息并将身份信息发送给 HN 进行身份验证, HN 接收到 SN 发送信息, 验证 UE 的身份信息, 并给 SN 发送质询消息.

```
if SN 未结束 and 满足条件 2 and 第 1 阶段结束 and Message3 未发送
do 发送 Message3
if SN 未结束 and 满足条件 4 and 第 1 阶段结束 and Message4 被攻击
do SN 结束
```

第 3 阶段 SN 接收到 HN 返回的质询消息, 将质询消息发送给 UE, UE 接收到质询消息, 首先验证其有效性, 若有效, 则将响应发送给 SN.

```
if SN 未结束 and 满足条件 4 and 第 1 阶段结束 and 第 2 阶段结束 and Message3 未发送
do 发送 Message3
if SN 未结束 and 满足条件 6 and 第 1 阶段结束 and 第 2 阶段结束 and Message6 被攻击
do SN 结束
```

第 4 阶段 SN 接收到 UE 的响应, 将响应发送给 HN, HN 对响应进行认证, 若符合, 则表示用户认证成功, 可以接入网络.

```
if SN 未结束 and 满足条件 6 and 第 1 阶段结束 and 第 2 阶段结束 and 第 3 阶段结束 and Message7 未发送
do 发送 Message7
if SN 未结束 and 满足条件 7 and 第 1 阶段结束 and 第 2 阶段结束 and 第 3 阶段结束 and Message8 被攻击
do SN 结束
```

4.2 AKA 协议属性的验证与分析

本节就 AKA 协议的时延性, 有效性, 保密性属性进行定量的分析.

4.2.1 时延性验证与分析

时延性是指 UE 终端设备在发送接入网络请求并且得到了 HN 归属域网络的验证, 且各模块均正常工作, 但用户终端设备因为外界对 UE 与 SN 通信或者 SN 与 HN 通信的攻击, 造成终端设备一直处于认证的状态, 而无法马上接入网络. 将协议正常工作描述为:

label"normal_work"=(UE&SN&HN)&(Message1–Message8)&(CheckMessage1–CheckMessage8)

其中, (UE&SN&HN) 表示 3 个模块均正常工作, (Message1–Message8)&(CheckMessage1–CheckMessage8) 表示每一阶段 3 个模块均发送过请求, 且请求信息和响应信息都是完整的, SendMessage8 & (CheckMessage8=1) 表示最后一次 SN 发送过请求信息, HN 正常响应了 SN 的信息.

验证的时延性表示为:

(1 – filter(state, P =?[F"normal_work"], "init"))

当把 attackNH 设为 0.3 时, 得到随着 attackES 攻击率增大, 协议满足时延性的概率变化结果, 横轴是 attackES 的概率取值, 竖轴是 attackES 和 attackNH=0.3 概率的攻击下协议满足时延性的概率, 如图 3 所示.

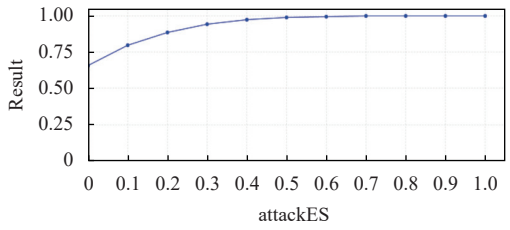

图 3 协议随 attackES 变化的时延性的概率情况 (attackNH=0.3)

试验结果表明, 当 attackES=0, attackNH=0.3 时, 协议满足时延性的概率为 0.657. 如图 4 所示, 当 attackES 攻击率为 1 时, 协议满足时延性的概率为 1, 即此时用户终端设备无法接入网络的概率为 1. 因此, 在外部攻击逐渐增大的情况下, 协议的时延性增大.

4.2.2 有效性验证与分析

协议的有效性指的是在所有模块正常工作时, 用户终端设备在发送请求并且得到认证成功的响应之后, 用户终端设备能够接入网络的性质. 有效性描述如下:

label"effective"=(CheckMessage2=1&CheckMessage5=1&FinishUE)&(CheckMessage1=1&CheckMessage4=1 & CheckMessage6=1 & CheckMessage8=1 & FinishSN) & (CheckMessage3=1 & CheckMessage7=1 & FinishHN) & con8;

其中, (CheckMessage2=1 & CheckMessage5=1 & FinishUE) 表示 UE 模块正常结束且接收到的信息也都是完整的, SN 和 HN 模块也都正常结束且收到的信息都是完整的.

有效性性质的状态概率描述为:

filter(state, P =?[F"effective"], "init")

对 attackES 和 attackNH 赋予不同的攻击概率, 得到图 5 的有效性随攻击概率变化的情况.

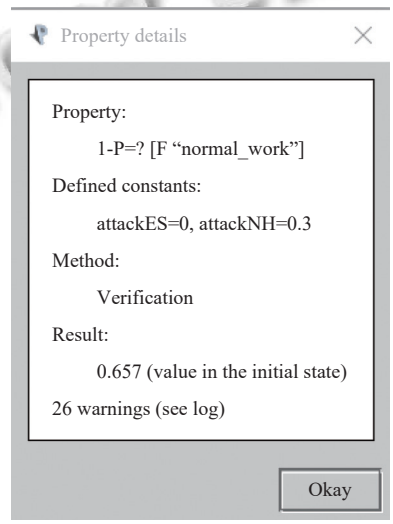

图 4 协议满足时延性的概率

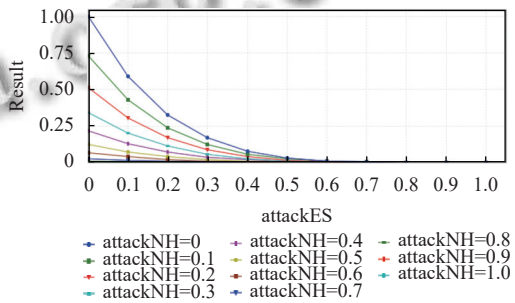

图 5 协议随攻击率改变而满足有效性的概率

当 attackNH 和 attackES 的取值都为 0 时, 即攻击的概率都为 0 时, 协议满足有效性的概率为 1, 当 attackES=0 时, 由图 5 得到随着 attackNH 的增大, 协议满足有效性的概率逐渐减小.

以 attackNH=0.1 曲线和 attackES 曲线的对比实验为例, 当 attackES=0.1, attackNH 在 (0, 0.1) 时, 协议满足有效性的概率小于 attackNH=0.1, attackES 在 (0, 0.1)

时协议满足有效性的概率; 当 attackES=0.1, attackNH 在 (0.1, 1) 时, 协议满足有效性的概率大于 attackNH=0.1, attackES 在 (0.1, 1) 时协议满足有效性的概率. 因此协议的有效性在 (0.1, 1) 间受 attackES 影响大, 有效性受 attackNH 攻击的影响更小, 在 (0.1, 1) 间受 attackES 影响小, 有效性受 attackNH 攻击的影响更大, 如图 6 所示.

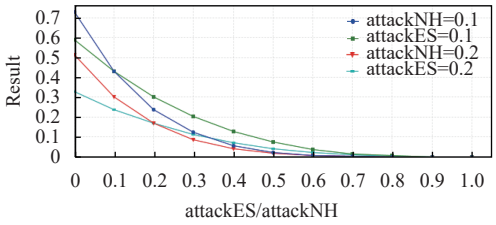

图 6 对比实验结果

推广到其他对比实验可以发现, 当 attackES 小于 attackNH 时, 协议此时有效性受 attackNH 影响更大; 当 attackES 大于 attackNH 时, 协议此时有效性受 attackES 影响更大, AKA 协议在实验环境中, 不同组合的攻击对 AKA 协议有效性的影响程度不同, 实际网络环境与实验网络环境相比更加复杂, UE 和 SN 之间是通过无线信道传递信息的, 很容易被攻击者破坏信息传递[12], 需要注重无线通信的保护.

4.2.3 保密性验证与分析

协议的保密性指的是用户终端设备在认证过程中信息不被泄漏的特性, 首先泄漏的特性描述为 label "non_confidential"=(FinishUE&((con2&CheckMessage2!=1) | (con5 & CheckMessage5!=1))) | (FinishSN & ((con1 & CheckMessage1!=1) | (con4 & CheckMessage4!=1) | (con6 & CheckMessage6!=1))) | (FinishHN & ((con3 & CheckMessage3!=1) | (con7 & CheckMessage7!=1))) 表示 3 个模块正常结束, 模块之间的请求信息全部发送, 但每次响应消息至少有一条是不完整的, 即信息是被截取了. 由上述对泄漏的特性的描述, 对保密性的状态概率的描述则为:

$$(1-\text{filter}(\text{state},P=?[F\text{“non\_confidential”}],\text{“init”}))$$

给 attackNH 设置为 0.3 时, attackES 攻击的概率与协议的保密性的关系如图 7 所示, 当 attackES 的攻击的概率逐渐增大时, 协议的保密性逐渐减小, 当 attackES 的攻击率为 1 时, 协议保密性为 0, 即协议的消息被攻击后泄漏.

当设置 attackNH=0.3, attackES=0 时, 协议满足的保密性概率为 0.49.

给 attackES 和 attackNH 设置不同的攻击概率得到如图 8 所示的结果.

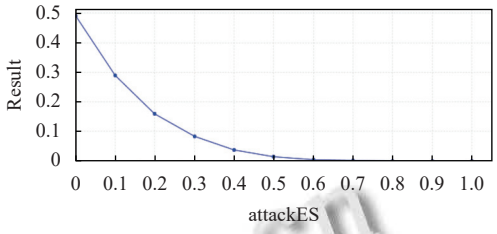

图 7 协议保密性随 attackES 变化情况 (attackNH=0.3)

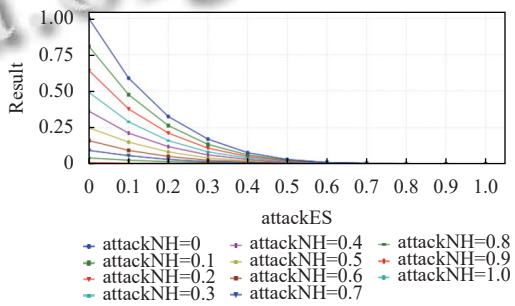

图 8 attackES 和 attackNH 不同取值对协议保密性影响情况

试验结果说明, 当设置 attackES=0, attackNH=0 时, 协议保密性的概率为 1, 即当外界不存在攻击时, 协议满足保密性的概率为 1, 当设置 attackES 和 attackNH 攻击的概率增大时, 协议满足保密性的概率逐渐降低, 且 attackES 与 attackNH 其中一个攻击概率达到 1 时, 协议满足保密性的概率为 0.

综合以上的实验结果, 实验表明该协议所验证的时延性, 有效性, 保密性均随着 attackES 和 attackNH 的增大而减小. 随着 attackES 和 attackNH 攻击增大, 协议的时延性, 有效性, 保密性不再满足性能要求.

5 结束与展望

本文以 5G 网络 AKA 协议为研究对象, 首先描述了 AKA 协议的大致执行流程, 通过对协议建立 DTMC 马尔科夫模型, 然后考虑在实际网络环境存在各种各样的网络攻击在模型中引入了描述外界影响的攻击概率, 通过使用 PRISM 模型检测器来建立系统的离散的状态和行为, 使用 PCTL 概率计算树逻辑对要验证的时延性, 有效性, 保密性进行描述, 通过实验对核心性质进行定量的研究和分析. 实验结果验证了协议存在

的缺陷, 在所受外部攻击增大时, 所验证的时延性, 有效性, 保密性不再满足要求. 本实验仍然存在一些不足之处, 即如何对协议缺陷进行改进, 使协议受到攻击之后还能满足性能要求. 接下来的工作是改进协议, 使时延性, 有效性, 保密性保持可靠的性能.

参考文献

1 邱勤, 张滨, 吕欣. 5G 安全需求与标准体系研究. 信息安全研究, 2020, 6(8): 673–679. [doi: 10.3969/j.issn.2096-1057.2020.08.002]

2 胡鑫鑫, 刘彩霞, 彭亚斌, 等. 5G 鉴权认证协议的安全性研究. 无线电通信技术, 2020, 46(4): 405–411. [doi: 10.3969/j.issn.1003-3114.2020.04.006]

3 齐旻鹏, 彭晋. 5G 网络的认证体系. 中兴通讯技术, 2019, 25(4): 14–18. [doi: 10.12142/ZTETJ.201904003]

4 陆峰, 郑康锋, 钮心忻, 等. 3GPP 认证与密钥协商协议安全性分析. 软件学报, 2010, 21(7): 1768–1782.

5 纪韬. 5G 网络中身份认证协议研究 [硕士学位论文]. 西安: 西安电子科技大学, 2018.

6 Arapinis M, Mancini L, Ritter E, *et al*. New privacy issues in mobile telephony: Fix and verification. Proceedings of the 2012 ACM Conference on Computer and Communications Security. North Carolina: ACM, 2012. 205–216.

7 Borgaonkar R, Hirschi L, Park S, *et al*. New privacy threat on 3G, 4G, and upcoming 5GAKA protocols. Proceedings on Privacy Enhancing Technologies, 2019, 2019(3): 108–127. [doi: 10.2478/popets-2019-0039]

8 Hahn C, Kwon H, Kim D, *et al*. A privacy threat in 4th generation mobile telephony and its countermeasure. Proceedings of the 9th International Conference on Wireless Algorithms, Systems, and Applications. Harbin: Springer, 2014. 624–635.

9 Hussain SR, Chowdhury O, Mehnaz S, *et al*. LTEInspector: A systematic approach for adversarial testing of 4G LTE. Proceedings of the 25th Annual Network and Distributed System Security Symposium. San Diego: The Internet Society, 2018.

10 Basin D, Dreier J, Hirschi L, *et al*. A formal analysis of 5G authentication. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto: ACM, 2018. 1383–1396.

11 Koutsos A. The 5GAKA authentication protocol privacy. Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P). Stockholm: IEEE, 2019. 464–479.

12 李晓逸. 5G 认证协议设计及形式化验证 [硕士学位论文]. 北京: 北京交通大学, 2021. [doi: 10.26944/d.cnki.gbfju.2021.000411]

13 Ferrag MA, Maglaras L, Argyriou A, *et al*. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 2018, 101: 55–82. [doi: 10.1016/j.jnca.2017.10.017]

14 夏奴奴, 杨晋吉, 赵淦森, 等. 基于概率模型的云辅助的轻量级无证书认证协议的形式化验证. 计算机科学, 2019, 46(8): 206-211. [doi: 10.11896/j.issn.1002-137X.2019.08.034]

15 Kwiatkowska M, Norman G, Parker D. Advances and challenges of probabilistic model checking. Proceedings of the 2010 48th Annual Allerton Conference on Communication, Control, and Computing. Monticello: IEEE, 2010. 1691–1698.

16 Sharir M, Pnueli A, Hart S. Verification of probabilistic programs. SIAM Journal on Computing, 1984, 13(2): 292–314. [doi: 10.1137/0213021]

17 Liu LY, Hasan O, Tahar S. Formal reasoning about finite-state discrete-time Markov chains in HOL. Journal of Computer Science and Technology, 2013, 28(2): 217–231. [doi: 10.1007/s11390-013-1324-6]

18 Kwiatkowska M, Norman G, Parker D. PRISM 4.0: Verification of probabilistic real-time systems. Proceedings of the 23rd International Conference on Computer Aided Verification. Snowbird: Springer, 2011. 585–591.

(校对责编: 孙君艳)