计算机科学
COMPUTER SCIENCE

EAP-TLS协议的形式化验证研究

陈丽萍，徐鹏，王丹琛，徐扬

引用本文

陈丽萍，徐鹏，王丹琛，徐扬.EAP-TLS协议的形式化验证研究[J]．计算机科学, 2022, 49(11A): 211100111-5.

CHEN Li-ping, XU Peng, WANG Dan-chen, XU Yang. Study on Formal Verification of EAP-TLS Protocol [J]. Computer Science, 2022, 49(11A): 211100111-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.211100111

EAP-TLS 协议的形式化验证研究

陈丽萍[1,2]　徐　鹏[1,2]　王丹琛[2,3]　徐　扬[1,2]
1 西南交通大学数学学院　成都 611756
2 系统可信性自动验证国家地方联合工程实验室　成都 611756
3 四川省数字经济研究中心　成都 610021
(1432652087@qq.com)

摘　要　EAP-TLS是5G标准定义的在特定物联网环境中提供密钥服务的安全协议,然而EAP-TLS协议无法提供用户设备与网络之间的双向认证,存在设计缺陷的协议在运行时将危害系统安全,因此在协议实施之前分析其安全性,尽可能找到潜在缺陷并将其改进是所有协议必不可少的过程。文中研究了基于Proverif的EAP-TLS协议与安全属性的形式化模型,并验证了用户设备与网络之间的相互认证性、协议中安全锚点密钥KSEAF与用户身份标识SUPI的保密性等安全属性。实验结果表明,在非安全信道下EAP-TLS协议在认证性方面存在安全缺陷,用户设备对网络的认证失败。分析验证结果进一步确定了导致安全缺陷的原因,并给出了相应的攻击路径。最后,基于密码学中的非对称密钥加密与随机数,讨论了安全缺陷改进的可能性。

关键词:认证协议;EAP-TLS;形式化验证;Proverif;非安全信道
中图法分类号　TN915.04

Study on Formal Verification of EAP-TLS Protocol

CHEN Li-ping[1,2],XU Peng[1,2],WANG Dan-chen[2,3] and XU Yang[1,2]
1 School of Mathematics,Southwest Jiaotong University,Chengdu 611756,China
2 National-local Joint Engineering Lab of System Credibility Automatic Verification,Chengdu 611756,China
3 Sichuan Provinical Digital Economy Research Center,Chengdu 610021,China

Abstract　EAP-TLS is a security protocol defined under the 5G standard that provides key services in a specific IoT environment. However,the EAP-TLS protocol cannot provide mutual authentication between user equipment and the network. A protocol with design flaws will endanger the security of the system during operation. Therefore,it is a very necessary process to analyze its security before the implementation of the protocol,try to find potential flaws and improve them. This paper studies the formal model of EAP-TLS protocol and security properties based on Proverif,and verifies the security properties such as the mutual authentication between user equipment and network,confidentiality between KSEAF(security anchor key) and subscriber permanent identity(SUPI). Verification results find that there are some security flaws in the EAP-TLS protocol in terms of authentication under insecure channels,and the user equipment fails to authenticate the network. Analytical results further confirm the reasons of security flaws,and the corresponding attacks are also given. Finally,the possibility of improving security flaws is discussed based on asymmetric key encryption and random numbers in cryptography.

Keywords　Authentication protocol,EAP-TLS,Formal verification,Proverif,Insecure channel

1　引言

随着各种新型网络安全风险的不断出现,在接入网、核心网、多种应用场景、网络能力开放等方面不断出现新的威胁。传统的网络安全风险和漏洞依然存在,新的安全攻击方式持续增加。5G安全机制除了要满足基本通信安全要求之外,还需要为不同业务场景提供差异化的安全服务,要能够适应多种网络接入方式及新型网络架构,保护用户隐私。

面对多种应用场景和业务需求,5G需要一个统一认证框架,用来支持多种应用场景的网络接入认证。EAP[1]认证框架是目前所知最能满足5G统一认证需求的备选方案。EAP具有很普遍的适用性,支持多种认证协议,如EAP-TLS,EAP-AKA,EAP-AKA′等。EAP-TLS[2]规范定义了EAP传输层安全性,其中包括对基于证书的相互身份认证和密钥派生的支持。认证和密钥协商过程的目的是使用户设备与网络之间能够相互身份验证,并提供可以在后续安全性过程中在

基金项目:国家自然科学基金(61976130);四川省科技计划项目(2020YJ0270);中央高校基本科研业务费专项资金(2682021GF012);四川省无线电监测站科研计划([2019]4)
This work was supported by the National Natural Science Foundation of China(61976130),Sichuan Province Science and Technology Planning Project(2020YJ0270),Fundamental Research Funds for the Central Universities(2682021GF012) and Scientific Research Plan of Sichuan Radio Monitoring Station([2019]4).
通信作者:徐鹏(pengxup@swjtu.edu.cn)

用户设备 UE 与网络之间使用的密钥材料。

安全协议本身可能存在设计漏洞，这可能导致它无法达到预期的安全目标，甚至在实施时危害系统安全。因此，分析协议的安全性，尽可能找到潜在缺陷并改进是非常必要的。已有文献对 EAP-TLS 协议中潜在的安全性问题进行了研究。Shojaie 等[3]对 EAP-TLS 进行分析，提出了一种具有离散密码机制和不同握手结构的增强方法，提高了协议的安全性，并缩短了执行时间。Zhao 等[4]分析了 EAP-TLS 中存在中间人攻击、拒绝服务等安全缺陷，并针对这些缺陷提出了改进方案。Zhang 等[5]使用 Scyther 对 EAP-TLS 协议进行形式化建模，验证了安全锚点密钥 KSEAF、用户身份标识 SUPI 的秘密性等安全属性，确定了该协议中几个可能危及安全性的设计缺陷。Zhang 等[6]使用 Proverif 对 EAP-TLS 协议进行形式化建模，验证了用户身份标识 SUPI、预主密钥 Rprekey、会话密钥 Ksession 的保密性，以及 UE 与 AUSF 之间的相互认证性和 UE 与 AUSF 对 Rprekey 的认证等安全属性，发现了对认证性的攻击，并针对攻击提出了相应的解决方案。分析相关研究工作发现，当前对于 EAP-TLS 协议的安全性研究，缺乏形式化验证，或仅在安全信道下进行形式化验证。

由于物理上的安全信道往往资源受限或成本太高或使用受限，通常不适合大范围使用，因此完美的安全信道通常在现实中不存在。安全协议的设计正是为了在复杂的网络环境中实现安全通信，因此协议的参与方应在开放、不安全的信道中也能保证通信安全。目前对安全协议的安全性分析方法主要是通过协议形式化分析与验证[7]来实现。形式化方法能有效利用数学或逻辑模型来分析系统及条件，从而验证系统在满足条件的情况下所得的证明是否正确。

基于此，本文研究非安全信道下 EAP-TLS 协议的形式化分析与验证，这里的非安全信道通常就是共用信道，例如互联网。首先将协议参与方简化为 UE，SN，HN 3 个实体，进一步对协议进行形式化建模；然后对 KSEAF，SUPI 的保密性以及 UE 与 HN 之间的相互认证等安全属性进行形式化描述。采用 Proverif[8]分析 EAP-TLS 协议，发现该协议在认证性方面存在安全缺陷。最后，基于非对称密钥加密与随机数对存在的安全缺陷进行改进，分析了协议参与方在认证时如何识别攻击者，进一步对改进后的协议进行形式化分析验证。

2 EAP-TLS 协议

EAP-TLS 协议是针对传输层且基于证书的双向认证安全协议。下文将结合 3GPP 文档 TS 33.501[2]与 RFC 5246[9]中的相关介绍，给出 EAP-TLS 协议交互过程的描述。本文中所涉及的部分缩略语[10-11]如表 1 所列。

表 1 缩略语对照

Table 1 Abbreviation comparison

Abbreviation	Description
UE	User Equipment
SN	Server Network
HN	Home Network
SEAF	Security Anchor Function
AUSF	AUthentication Security Function
UDM	Unified Data Management
SUPI	Subscriber Permanent Identity
SUCI	Subscription Concealed Identifier

EAP-TLS 认证的流程如图 1 所示，主要包括以下 4 个阶段。

(1)初始准备阶段。在此阶段，用户设备 UE 发送含用户身份标识 SUCI 的请求认证消息(用 UDM 的公钥加密 SUPI 后得到 SUCI)，SEAF 将此消息与服务网络名称 SN-name 发送给归属网络 HN。在 HN 对 UE 的身份标识进行验证通过后，选择认证方法 EAP-TLS，并经 SEAF 将方法标识发送给 UE，随后 UE 经 SEAF 向 HN 发送响应消息 TLS Client-hello。

(2)UE 认证 HN。HN 经 SEAF 向 UE 发送服务器证书 Server-Certificate 以及请求客户端提供证书 Certificate-request 等消息。在接收到这些消息后，UE 通过服务器证书验证 HN 的身份。

(3)HN 认证 UE。UE 经 SEAF 向 HN 发送客户端证书 Client-Certificate 以及 Client-key-change，Client-Certificate-verif 等消息。HN 通过客户端证书验证 UE 的身份。

(4)安全锚点密钥 KSEAF 的生成。在 HN 经 SEAF 向 UE 发送响应消息 change-cipher-spec 与 Server-finished，UE 经 SEAF 向 HN 发送 EAP-TLS 之后，HN 由主密钥 master secret 生成 KSEAF，并将其与 EAP-Success 一同发送给 SEAF。SEAF 将 EAP-Success 转发给 UE，UE 按照与 HN 同样的方法生成 KSEAF 用于后续的通信。

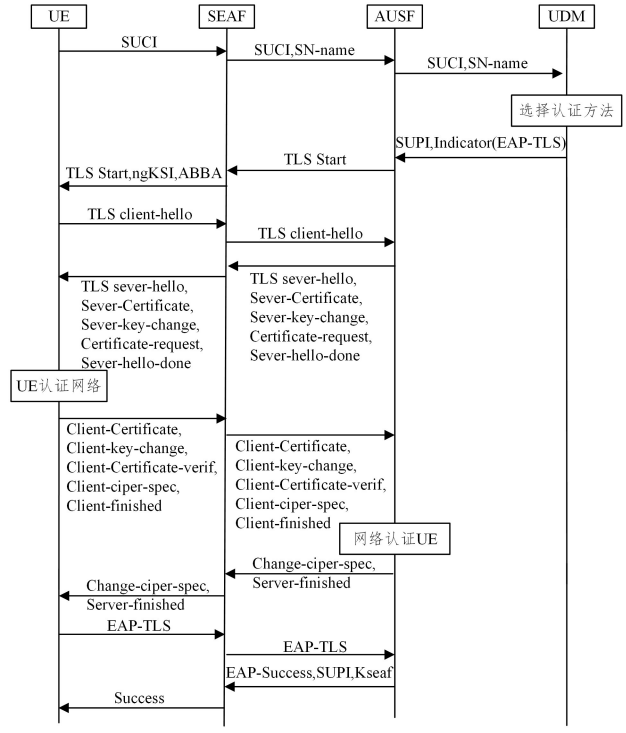

图 1 EAP-TLS 认证流程

Fig. 1 Authentication procedures of EAP-TLS

在以上的认证流程中，SEAF 为 SN 的关键模块，主要转发 UE 与 HN 之间的消息。另外，HN 由 AUSF 与 UDM 两部分组成，其中 AUSF 负责认证，UDM 负责数据管理。在 UE 与 HN 相互认证的过程中，UE 与 HN 均会获得主密钥 master secret。master secret 由 Client-key-change 中包含的 premaster secret、Client-hello 中的客户端随机数以及 Server-hello 中的服务器随机数生成。由于篇幅有限，认证流程中握手消息的具体内容没有完全给出，详细内容在 RFC 5246 中定义。

3 EAP-TLS 协议非安全信道模型

安全协议使协议参与方在开放、不安全的信道中完成密钥协商和相互认证，则应保证 EAP-TLS 协议在不安全信道下也能满足安全需求。

3.1 参与方模型

EAP-TLS 协议交互过程中涉及 4 个参与方：UE，SEAF，AUSF 和 UDM。其中 SEAF 为 SN 的关键模块，它在用户设备与归属网络之间的身份验证过程中充当“中间人”，在用户设备和归属地网络之间转发消息。AUSF 和 UDM 为 HN 的两个关键模块，AUSF 对用户设备进行认证，UDM 承载数据管理相关功能。由于协议中 UDM 部分只涉及对 SUCI 的解密以及认证方法的选取，因此可将协议的参与方简化为 3 个实体，即 UE，SN，HN（HN 包括 AUSF 和 UDM 两部分），从而简化协议的建模。

3.2 基于 Proverif 的形式化模型

Proverif 是基于应用 Pi 演算[12]的进程代数开发的安全协议验证器，建模过程所涉及的部分表达式及其含义如表 2 所列。

表 2 表达式及含义

Table 2 Expression and meaning

Expression	Description
free n：t.	declares the free namen of type t
type t.	declares user-defifined types
fun $f(t_1,\cdots,t_n):t$.	constructor(function symbols)
reduc for all $x_1:t_1,\cdots,x_n:t_n$; $f(x_1,\cdots,x_n)=m$.	destructor
new $n:t$;	namerestriction
in(c,$x:t$);	messageinput
out(c,x);	messageoutput
let $x=M$ in	term evaluation
!P	replication
P|Q	parallel composition

构建协议的形式化模型，主要包括对信道、密码学原语、各参与方在信道上发送与接收消息的形式化描述。将密码学原语中的关系抽象成函数来表达，协议参与方发送与接收的消息用变量以及函数来表达。协议的形式化建模主要包括以下几个部分。

（1）信道声明。将 UE 与 SN、SN 与 HN 之间的信道建模为不安全型（公开型）的 c_1，c_2。

（2）类型声明。Proverif 内置类型有限，在建模时可以根据需要自定义变量类型。如协议中涉及非对称密钥加密，因此需要用到公钥与私钥，则可自定义变量类型 pkey 表示公钥，skey 表示私钥。

（3）函数声明。声明函数 aenc，adec，sign，checksign，pk 分别表示加密、解密、签名、验证签名、由私钥获取相应公钥。其中，解密函数 adec 需要用析构函数来声明，因为解密函数 adec 与加密函数 aenc 相关，必须保证用私钥解密后的内容与对应公钥所加密的内容一致。另外，这些函数不涉及具体运算，只是形式地定义变量之间的关系。

（4）子进程声明。声明子进程 UE，SN，HN 来对协议中 UE，SN，HN 的行为进行建模，包括生成、发送、接收以及验证消息等行为。

（5）主进程声明。主进程相当于编程语言中的 main 函数。主进程主要包括 3 个部分：1）声明私钥；2）利用私钥获取公钥，并在信道 c_1，c_2 上发送公钥（使攻击者可以获取公钥）；3）复制并行 UE，SN 与 HN 进程。因为在运行协议时可能存在攻击者对其发起攻击，攻击者可以通过多次运行协议来进行攻击，因此需要复制并行各子进程。

完整的协议形式化描述较冗长，以下仅给出部分描述。

（1）信道声明

free c1：channel.

（2）类型声明

type pkey.

（3）函数声明

fun pk(skey)：pkey. //由私钥获取相应公钥

fun aenc(bitstring，pkey)：bitstring. //公钥加密

reduc forall m：bitstring，sk：skey；adec(aenc(m，pk(sk))，sk)＝m. //私钥解密

（4）子进程声明

以子进程 SN 为例，对 SN 的建模即协议中与 SN 相关行为的应用 pi 演算进行描述。

let SN＝

in(c_1，SUCI：bitstring)；//等待来自信道 c_1 的类型为 bitstring 的消息 SUCI

out(c_2，(SUCI，SEAFN))；//在 c_2 信道上发送消息 SUCI 与 SEAFN

……

in(c_2，(Success：bitstring，SUPIx：bitstring，KSEAF：bitstring))；

out(c_1，Success).

（5）主进程声明

process

new skUE：skey；//私钥声明

……

let pkUE＝pk(skUE) in//由私钥获取相应公钥

……

out（c_1，（pkUE，pkAUSF，pkUDM，spkAUSF，spkUE））；//在信道 c_1 上发送公钥

out(c_2，(pkUE，pkAUSF，pkUDM，spkAUSF，spkUE))；

((!UE(pkAUSF，pkUDM，sskUE)) |(!SN) |(!HN(skAUSF，spkUE，skUDM))) //复制并行子进程 UE，SN 与 HN

3.3 攻击模型

本文采用 Dolev-Yao 敌手模型[13]，在此敌手模型中假设存在攻击者能控制整个网络，发起主动攻击与被动攻击。攻击者具有如下的能力。

（1）攻击者可以窃听和拦截公共信道中传输的消息。

（2）攻击者可以在公共信道中发送拦截到的或自己构造的消息。

（3）攻击者可以作为合法主体参与协议的运行。

另外，攻击者满足完美密码学假设，即攻击者只有在知道相应密钥的情况下才能解密消息。

3.4 安全属性模型

以下将给出待验证的安全属性[14-15]。EAP-TLS 认证协议应提供用户与归属网络之间的相互认证。当他们就彼此的

身份达成一致时，才能实现他们之间的相互认证。因此，将此安全需求解释为身份认证属性：在协议成功终止后，UE 与 HN 都应该就彼此的身份达成一致。

5G 网络提供对用户的隐私保护，其中包括对身份标识的保护。由于密钥 KSEAF 被用于保护用户设备和网络之间的后续通信，因此应当保证 KSEAF 的秘密性。另外，主密钥 master secret 用于生成 KSEAF，但这里不考虑主密钥的保密性，而考虑预主密钥 prekey（即之前的 premaster secret）的保密性。因为 UE 与 HN 由预主密钥、客户端随机数、服务器随机数生成主密钥，所以主密钥不需要在信道上传送。然而预主密钥 prekey 由 UE 生成，并用 HN 的公钥加密后经 SEAF 发送给 HN，用于后续主密钥的生成以及 KSEAF 的生成，因此需要保证 prekey 的秘密性。将保密需求解释为以下的保密属性。

(1)攻击者无法获取到用户身份标识 SUPI。

(2)攻击者无法获取到安全锚点密钥 KSEAF。

(3)攻击者无法获取到预主密钥 prekey。

对上述保密性及认证性的形式化表述如表 3 所列。其中，query attacker(M)用于验证 M 的保密性，query $x_1:t_1,\cdots,x_n:t_n$；inj-event($e_1(m_1,\cdots,m_j)$) ==> inj-event($e_2(n_1,\cdots,n_k)$)用于验证认证性。

表 3 安全属性形式化描述

Table 3 Formal description of security properties

Security Property	Query
Confidentiality	query attacker(SUPI) query attacker(KSEAF) query attacker(prekey)
Authentication	query x: bitstring; inj-event(termAUSF(RUE)) ==> inj-event(acceptsUE(RUE)) query x1: bitstring, x2: bitstring; inj-event(termUE(Start, Rausf)) ==> inj-event(acceptsAUSF(Start, Rausf)).

4 验证结果及分析

在配置为 I5/16G/1TB 的计算机上使用 Proverif 2.02 验证非安全信道下的形式化模型。

4.1 验证结果

在对协议和安全属性形式化建模后，使用 Proverif 对其进行验证，验证结果如图 2 所示。分析验证结果发现，在不安全信道下，协议不能满足上述的安全需求。协议虽然能满足用户身份标识 SUPI、密钥 KSEAF、预主密钥 prekey 的保密性以及 HN 对 UE 的认证，但 UE 对 HN 的认证失败。

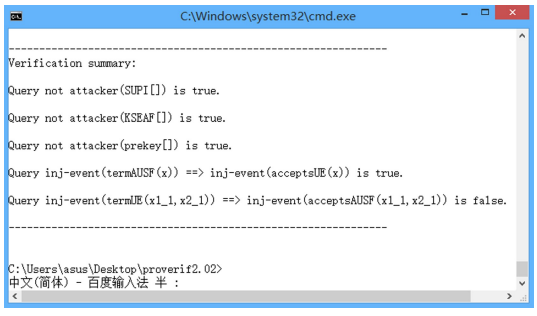

图 2 验证结果

Fig. 2 Verification results

4.2 攻击分析

使用 Proverif 对协议与安全属性的形式化模型进行验证，验证失败时 Proverif 会提供相应的失败信息。

分析相应信息，发现存在中间人攻击，导致 UE 对 HN 认证失败的攻击具体如图 3 所示。以明文方式发送消息 Start，Rausf，Success，导致攻击者可以截获到这些消息，并替换为自己生成的消息 Start'，Rausf'，Success'再发送给 UE。攻击者可以冒充 HN 与 UE 建立连接，但 UE 无法识别这些消息来自 HN 还是攻击者，从而导致认证失败。

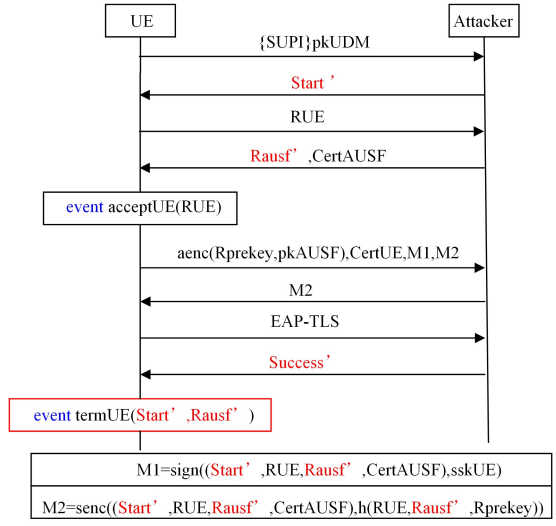

图 3 攻击流程

Fig. 3 Attack procedures

5 EAP-TLS 改进讨论

5.1 改进讨论

通过上述分析发现，UE 不能识别消息 Start，Rausf，Success 是否来自 HN，进而导致认证失败。直观的解决方案是将 HN 发送的消息加上标识。因此，考虑在发送这些消息时添加一个保密数据，同时在发送这些消息时采用非对称密钥进行加密。

为避免攻击者获取到 Start，Rausf，Success，并替换为 Start'，Rausf'，Success'后发送给 UE，考虑在发送 Start，Rausf，Success 时添加一个标识，并采用非对称密钥加密后再发送这些消息。若不采用加密，以明文的方式发送消息，则攻击者可以获取到标识，进一步发送替换后的消息与标识，从而接收方无法通过标识来判别消息是否被替换。若仅采用加密而不添加标识，则攻击者可用公钥加密替换后的消息再发送，接收方用私钥解密消息后仍然不能判别消息是否被替换。因此，考虑在添加标识的同时采用非对称密钥加密，加密后的标识只有发送方以及私钥拥有者才能获取，从而它们可以通过该标识来判别所接收的消息是否被替换。

采用对称密钥加密时，消息发送方与接收方使用相同的密钥，协商密钥时容易被泄露，存在密钥协商与交换问题，因此采用非对称密钥加密。非对称密钥加密的加密与解密使用不同密钥（公钥与私钥），私钥保密，公钥公开，攻击者只有在获取到相应私钥的情况下，才能解密由对应公钥加密的消息。由于仅在信道上发送公钥，攻击者不能获取到私钥，因此使用公钥进行加密，只有私钥拥有者才能解密消息，从而避免攻击者获取到这些消息。

对 EAP-TLS 的具体改进如图 4 所示，其中 M6＝sign((Start,RUE,Rausf,CertAUSF),sskUE)，M7＝senc((Start,RUE,Rausf,CertAUSF),h(RUE,Rausf,Rprekey))，具体内容如下。

(1)UE 生成随机数 RAND，将 SUPI 与 RAND 用 UDM 的公钥 pkUDM 加密后经 SN 发送给 HN。通过加密将随机 RAND 发送给 HN，后续 HN 在发送消息时添加该标识，UE 可以通过判别 RAND 实现对 HN 的认证。

(2)HN 在发送 Start 时添加 RAND，并用 UE 的公钥 pkUE 加密后经 SN 发送给 UE。

(3)HN 在发送 Rasuf 时添加 RAND，并用 pkUE 加密后经 SN 发送给 UE。

(4)SN 在发送 Success 时添加 SUPI，并用 pkUE 加密后发送给 UE。

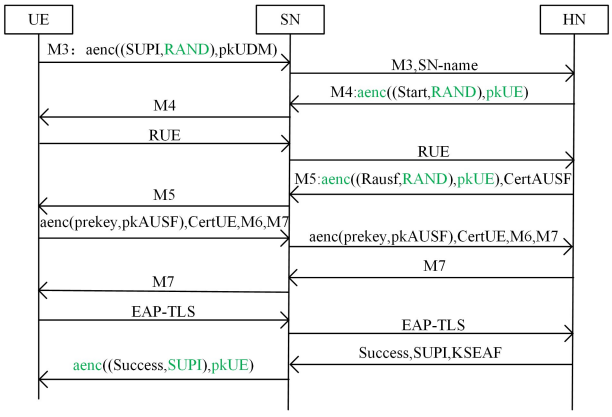

图 4　EAP-TLS 改进

Fig. 4　Improvement of EAP-TLS

5.2　有效性验证

下文将不改变之前所验证的安全属性，对改进方案进行形式化验证，验证结果如图 5 所示。分析验证结果发现，改进后的协议不仅可以满足 SUPI，KSEAF，prekey 的保密性以及 HN 对 UE 的认证，还能满足之前被违反的认证性。改进后 UE 成功对 HN 进行了认证，因此上述改进方案有效。

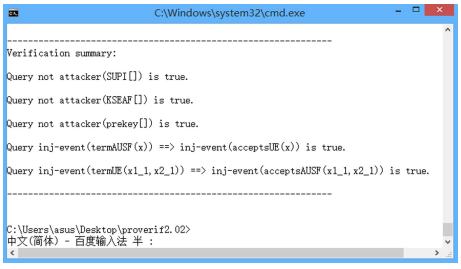

图 5　改进后的验证结果

Fig. 5　Improved verification results

结束语　5G 快速发展的同时也面临着越来越多的安全性问题，因此移动通信安全架构面临着更大的挑战。认证协议对于确保信息安全至关重要。本文使用形式化验证工具 Proverif 对 EAP-TLS 进行形式化验证，对验证结果进行分析，确定出具体的攻击，分析造成安全缺陷的原因，并基于密码学讨论了协议的改进。在改进过程中添加了新的加密项，增加了运算量与复杂度，后续工作可以结合效率进行研究。另外，EAP-TLS 交互过程较为复杂，可以进一步考虑在保证原有安全性的前提下，简化协议的交互过程，以及用到的加密方式及加密内容等。

参 考 文 献

[1] HUANG Z W. 5G network security practice [M]. Beijing: Posts & Telecom Press, 2020: 116-119.

[2] 3GPP. 3GPP TS 33.501 Security architecture and procedures for 5G system(Release 16)[S]. Nice: 3GPP, 2020.

[3] SHOJAIE B, SABERI I, SALLEH M. Enhancing EAP-TLS authentication protocol for IEEE 802.11i[J]. Wireless Networks, 2017, 23(5): 1491-1508.

[4] ZHAO Y H, QIAN Q. Research on Security Analysis and Improvement of EAP-TLS Protocol [J]. Software Guide, 2017, 16(8): 174-178.

[5] ZHANG J, WANG Q, YANG L, et al. Formal Verification of 5G-EAP-TLS Authentication Protocol[C]// 2019 IEEE Fourth International Conference on Data Science in Cyberspace(DSC). Hangzhou: IEEE, 2019: 503-509.

[6] ZHANG J, YANG L, CAO W, et al. Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif [J]. IEEE Access, 2020, 8: 23674-23688.

[7] TIAN J. Formal Verification [M]. Wiley-IEEE Press, 2005: 251-266.

[8] BLANCHET B. Modeling and Verifying Security Protocols with the Applied Pi Calculus and Proverif[M]. Now Foundations and Trends, 2016: 1-135.

[9] DIERKS T, RESCORLA E. The Transport Layer Security (TLS) Protocol Version 1.2 [EB/OL]. [2020-01-21]. https://datatracker.ietf.org/doc/rfc5246/.

[10] YANG Z Q, SU L, YANG B, et al. 5G Security Technology and Standards[M]. Beijing: Posts & Telecom Press, 2020: 275-289.

[11] HUANG Z W. 5G network security practice [M]. Beijing: Posts & Telecom Press, 2020: 331-332.

[12] RYAN M D, SMYTH B. Applied pi calculus[EB/OL]. [2021-11-08]. https://www.cs.bham.ac.uk/~mdr/research/papers/pdf/11-applied-pi.extended.pdf.

[13] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[14] FENG D G, XU J, LAN X. 5G mobile communication network security research[J]. Journal of Software, 2018, 29(6): 1813-1825.

[15] QIANG Q, WU G, HUANG K Z, et al. Progress in 5G security technology research and standards[J]. Scientia Sinica(Informationis), 2021, 51(3): 347-366.

CHEN Li-ping, born in 1997, postgraduate. Her main research interests include formal verification of security protocols and so on.

XU Peng, born in 1981, Ph.D, lecturer. His main research interests include cyberspace security, formal verification, spectrum and electromagnetic environment management.