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

夏奴奴 杨晋吉 赵淦森 莫晓珊
(华南师范大学计算机学院 广州 510631)

摘 要 匿名WBANs通信技术是保护互联网用户和服务器间隐私的最有力手段之一,但匿名WBANs无证书认证协议的形式化验证仍是亟待解决的难题。采用概率模型检测的方法对一种基于云辅助的匿名WBANs的轻量级无证书认证协议建立离散时间马尔科夫链模型,在协议建模的状态迁移中加入了攻击率,重点对攻击率进行定量分析,用概率计算树逻辑对协议属性进行描述,利用PRISM概率模型检验工具对协议进行定量分析和验证,并且与SIP协议进行性能方面的对比。验证结果表明:在匿名WBANs通信环境下,云辅助的轻量级无证书认证协议各实体间所受攻击率对协议的不可否认性、时延性和有效性有不同程度的影响,控制好攻击率可以提高协议安全性,这对医疗服务质量和实时监测效率的提高以及远程医学的基本需求有着极大的意义。

关键词 概率模型检测,WBANs,攻击率,云辅助的轻量级无证书认证协议,PRISM
中图法分类号 TP301 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.08.034

Formal Verification of Cloud-aided Lightweight Certificateless Authentication Protocol Based on Probabilistic Model

XIA Nu-nu YANG Jin-ji ZHAO Gan-sen MO Xiao-shan
(School of Computing, South China Normal University, Guangzhou 510631, China)

Abstract Anonymous wireless body area networks communication technology is one of the most powerful means to protect the privacy of Internet users and servers, but formal authentication of anonymous wireless body area networks certificateless authentication protocol is still a difficult problem to be solved. The method of probabilistic model detection is used to set up a discrete time Markov chain model based on a cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. The attack rate is added to the state migration of the protocol modeling, and in particular, the attack rate was analyzed quantitatively. The protocol attributes are described with the probability calculation tree logic, the PRISM namely a probabilistic model testing tool was used for quantitative analysis and verification of the protocol, and the performance of the protocol was compared with the SIP protocol. The result shows that the attack rate between the entities of the cloud-aided lightweight certificateless authentication protocol has different influence on non-repudiation, time delay and effectiveness of the protocol under anonymous WBANs communication environment. The control of the attack rate can improve the security of the protocol. It is of great significance to the quality of medical services, the improvement of real-time monitoring efficiency and the basic needs of telemedicine.

Keywords Probabilistic model checking, Wireless body area networks, Attack rate, Cloud-aided lightweight certificateless authentication protocol, PRISM

1 引言

随着云计算[1]和无线体域网(WBANs)[2]的发展,可穿戴设备能够成为新的智能终端,为用户提供服务,对用户改善人类医疗保健服务起着重要的作用。由于病人和消费者的需求增长,医疗数据也快速增长,因此需要及时处理感测的医疗数据,也需要医生的及时反馈。然而,传统WBANS的存储和计算能力较低,已经远不能满足实际应用的需求。为此,将云计算技术与传统的WBANS相结合,使其能够实时存储和处理感测的医学数据。但是,云计算环境的开放性和网络的复杂性使得云计算面临严重的安全威胁[2]。云辅助的轻量级无证书认证协议可以在不安全的信道提供更安全的隐私信息保护。因此,研究云辅助的轻量级无证书认证协议的安全性是一个很重要的课题,对人类的医疗保健等相关方面有着极大的意义。

到稿日期:2018-07-20 返修日期:2018-11-14

夏奴奴(1994—),女,硕士生,主要研究方向为模型检测、协议验证;**杨晋吉**(1968—),男,博士,教授,主要研究方向为模型检测、协议验证,E-mail:yangjj@scnu.edu.cn(通信作者);**赵淦森**(1977—),男,博士,主要研究方向为云计算、大数据;**莫晓珊**(1993—),女,硕士生,主要研究方向为模型检测、协议验证。

在开放的云计算环境中，数据信息在交换传输的过程中会遭受恶意实体的攻击，从而导致接收信息不完整或者丢失，因此引用攻击率对轻量级无证书认证协议的重要属性进行定量分析在实际场景中有着重要的意义。

目前，已有一些关于概率模型检测形式化验证和云计算安全协议方面的研究。文献[4]分析了建模为离散时间马尔可夫链的现有团队形成协议的性能，并且用概率模型检验工具 PRISM 验证了典型的概率规范。文献[5]通过引入概率抽象的新概念，并通过扩展模型检测的框架，验证了给定程序在所有输入上的正确性。文献[6]详细描述了如何在概率模型检查器棱镜中建模，并对检验该模型的定量属性的丰富选择进行了说明。文献[7]设计了一个云存储系统的审计框架，并提出了一个有效的隐私保护审计协议。文献[8]提出了一种可信移动终端云服务安全接入方案，并且利用 ARM Trust Zone 硬件隔离技术构建可信移动终端，保护云服务客户端及确保安全敏感操作在移动终端的安全执行。文献[9]提出了基于双服务器的带密文等值判定的公钥加密协议，并在随机预言机模型下证明了其安全性；同时，该文献还对设计的协议进行了性能分析。文献[10]提出了一个匿名的无线体域网络的云辅助轻量级无证书认证协议，虽然可信第三方完成了对平台的完整性验证，实现了终端用户和云服务器平台的身份双向认证，但是忽略了文件系统的安全问题，因此本文工作是对该协议进行形式化验证与分析。

本文首先对概率模型检测进行了简单的描述，然后对一种云辅助的轻量级无证书认证协议进行了形式化验证与分析，选用概率模型对协议进行建模，并使用概率计算树逻辑(Probabilistic Computation Tree Logic，PCTL)对协议重要属性进行定量描述，最后采用模型检测工具 PRISM 验证了该协议的重要属性，并且与 SIP 协议进行了性能对比。结果表明，这种云辅助的轻量级无证书认证协议的时延性、有效性和不可否认性都受攻击率的影响，对相应实体间攻击率进行控制可以提高协议安全性。

2　概率模型检测

概率模型检测(Probability Model Checking)[11]是一种形式化验证技术[12]，主要用来验证系统是否满足它所要求的一些性质。模型检测的方法一般是先对系统建立模型，这个模型一般是有限状态自动机，它的状态代表系统可能的配置。自 2005 年以来，已有多种随机模型检测器被提出，它们都可以自动生成马尔可夫模型，其中 PRISM[13]的应用最广泛。PRISM 是一种概率模型检查器，是一种用于显示概率行为的系统的建模和分析工具，它通过建立一个系统的精确数学模型进行分析，然后将该系统的属性在时序逻辑中正式表示，并对所构造的模型进行自动分析。PRISM 可以建立和分析 5 种类型的概率模型：离散马尔可夫链(Discrete-Time Markov Chain，DTMCs)、连续时间马尔可夫链(Continuous-Time Markov Chain，CTMCs)、马尔可夫的决策过程(Markov Decision Processes，MDP)、概率自动机(Probabilistic Automata，PAs)和概率时间自动机(Probabilistic Timed Automata，PTAS)。本文通过离散时间马尔可夫链对轻量级无证书认证协议进行形式化建模，然后通过概率计算树逻辑(PCTL)对轻量级无证书认证协议的核心属性进行定量分析。

2.1　离散时间马尔科夫链

离散时间马尔科夫链(Discrete Time Markov Chain，DTMC)[14]是一个四元组，$D=\langle S,\bar{s},\Delta,L\rangle$其中，$S$ 表示有穷状态集合；$\bar{s}$表示初始状态集合，对于任一状态集合 $s\in\bar{s}$，有 $s\in S$；Δ 表示 $S\times S\to[0,1]$，是一个迁移概率函数；L 表示 $S\to 2^{AP}$，是标记函数。

如图 1 所示，$S=\{\bar{s},s_1,s_2,s_3,s_4\}$是有穷状态集，其中包含初始状态$\bar{s}$，迁移概率函数 $\Delta(\bar{s},s_1)=0.2$ 表示从状态$\bar{s}$迁移到状态 s_1 的概率为 0.2。标记成功状态 s_4 为 $L(s_4)=\{succ\}$。

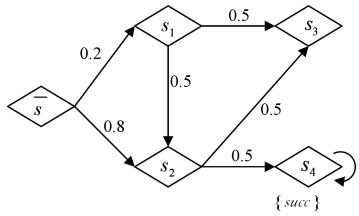

图 1　离散时间马尔可夫链实例图

Fig. 1　Simple of DTMC

2.2　概率计算树逻辑

概率计算树逻辑(PCTL)[15]是一个著名的概率时间逻辑，也是计算树逻辑(CTL)的扩展，它用来描述模型是否满足一个特定的形式化规格(或属性)，能够描述概率模型的定量属性。

以图 1 所示的离散时间马尔可夫链为例，它可以描述其最终达到成功状态的概率。例如：$P=[F\ succ]$。其结果可以在 PRISM 工具上运行并验证，结果表明该离散时间马尔可夫链最终达到成功状态的概率为 0.45。

3　基于攻击率的概率模型检测

本文在状态迁移中加入一个攻击率对云辅助的轻量级无证书认证协议的重要属性进行定量分析。本节首先针对云辅助的轻量级无证书认证协议的实体分别进行形式化建模，并且简要介绍基于随机模型检验的验证过程，对在建模过程中攻击率对协议产生的影响进行说明；然后基于攻击率定量分析云辅助的轻量级无证书认证协议的重要属性；最后将其与 SIP 协议进行性能方面的对比分析。

3.1　云辅助的轻量级无证书认证协议的形式化建模

该协议实体主要包含 WBAN 用户(WBAN User，WU)、云服务器(Cloud Server，CS)和网络管理者(Network Manager，NM)。NM 作为密钥生成中心，负责 WBAN 用户和应用程序提供商的注册，它类似于完全可信的第三方，管理整个网络和权限。通过对实体进行建模可以分析其是否满足云辅助的轻量级无证书认证协议的重要安全属性：时延性(Time ductility)、有效性(Effectiveness)和不可否认性(Non repudiation)。

如图 2 所示，WU 先与 NM 进行信息交互，然后 NM 再与 CS 进行信息传递，最后 WU 与 CS 进行信息确认。

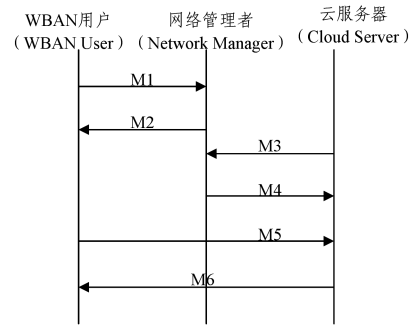

图 2 云辅助的轻量级无证书认证协议模型

Fig. 2 Cloud-aided lightweight certificateless authentication protocol model

为了对云辅助的轻量级无证书认证协议的重要属性进行自动化验证,本文使用模型检测工具 PRISM 对选用的一种基于云辅助的匿名无线体域网络的轻量级无证书认证协议进行形式化建模。首先通过离散时间马尔科夫链对整个协议阶段进行描述。

如图 3 所示,本文使用 PRISM 语言建立系统模型,在对任意一个系统建模之前,都需要对其形式化,以提高模型质量。一般通过设置随机模型检测器 PRISM 的某些参数和选项对其进行初始化并运行。随机模型检验给出的结果有 3 种:空间存储不足、满足性质和不满足性质并给出反例。满足性质是乐见其成的,对于其他两种结果,通常可以采取一些方法使结果往满足性质的方向发展,即向好的结果靠拢。表 1 列出了云辅助的轻量级无证书认证协议的代码符号。

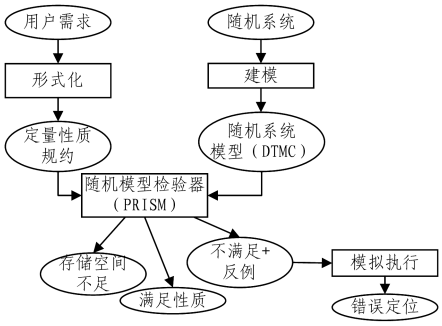

图 3 基于随机模型检验的验证过程

Fig. 3 Verification process based on random model test

表 1 符号说明

Table 1 Symbols' expression

符号	含义
SendMessagei	二值变量,false 表示消息 i 未被发送,true 表示消息 i 已被发送
checkMessagei	变量,0 表示消息 i 未检验,1 表示消息 i 完整,2 表示消息 i 不完整
stopX	二值变量,false 表示模块 X 正常运行,true 表示模块 X 选择终止协议
attackUC	实体 WU 与 CS 间所受攻击率
attackNM	实体 WU、CS 与 NM 间所受攻击率
flagj	二值变量,表示标志信号

云辅助的轻量级无证书认证协议主要分为 3 个阶段,分别为用户注册阶段、提供商注册阶段和服务阶段。

(1)用户注册阶段

M1 和 M2 为用户注册阶段。M1 表示注册请求,M2 表示注册请求响应。

每一步的信息接收方在接收信息后,通过检查信息是否完备选择下一步操作。例如,当 NM 收到 WU 发送的消息 1 后,先检查消息 1 是否完备。如果消息完备,则 NM 向 WU 发送消息 2;如果消息 1 不完备,那么 NM 选择终止协议。

[] !stopNM & sendMessage1 & (checkMessage1=0)& !sendMessage2−> attackNM:(checkMessage1′=2)+(1−attackNM):(checkMessage1′=1);

……

[] !stopNM & sendMessage1 & (checkMessage1=1)& !sendMessage2 −> 1:(sendMessage2′=true);

(2)提供商注册阶段

M3 和 M4 为提供商注册阶段。M3 表示注册请求,M4 表示注册请求响应。

[] !stopNM & sendMessage1 & sendMessage2 & sendMessage3 & (checkMessage3=0)& !sendMessage4−> attackNM:(checkMessage3′=2)+(1−attackNM):(checkMessage3′=1);

……

[]!stopCS & sendMessage1 & sendMessage2 & sendMessage3 & sendMessage4 & (checkMessage4= 1) & !flag2 −> 1:(flag2′=true);

(3)服务阶段

M5 至 M6 为服务阶段。M5 表示服务请求,M6 表示服务响应。

[] !stopUU & sendMessage1 & sendMessage2 & sendMessage3 & sendMessage4 & flag2 & !sendMessage5−> 1:(sendMessage5′=true);

……

[] !stopUU & sendMessage1 & sendMessage2 & sendMessage3 & sendMessage4 & sendMessage5 & sendMessage6 & flag2 & (checkMessage6= 1)−> 1:(stopUU′=true);

3.2 协议属性验证与分析

本节对云辅助的轻量级无证书认证协议的不可否认性、时延性和有效性进行定量分析。

不可否认性[16]保证执行服务用户不能否认自己享受的服务,而提供者不能否认他们为用户提供了特色的服务。因此可以把协议不可否认性描述为:

label "undeniable" = stopUU & stopNM & stopCS & (sendMessage2 & checkMessage2 = 1) & (sendMessage4 & checkMessage4=1)。其中,stopUU & stopNM & stopCS 是协议结束的标志;sendMessage2 & checkMessage2=1 表示网络管理者(NM)确认了对 WBAN 用户 WU 的身份认证;sendMessage4 & checkMessage4=1 表示网络管理者(NM)确认了对云服务器(CS)的身份认证。

通过定义 attackUC 和 attackNM 可以描述实体 WU、NM 和 CS 之间的攻击率。假设实体 WU 和 CS 间所受攻击率为 0.5。首先验证当实体 WU、CS 与 NM 间所受攻击率为 0.5 时,可信接入云安全协议满足不可否认性的情况,因此将 attackUC 和 attackNM 都设置为 0.5。

当使用 PRISM 验证模型属性时,默认情况下,将返回模

型初始状态的值。但由于实际需要，可以通过设置 filter 过滤器来同时计算所有状态的值。通过 PRISM 计算协议时限性的状态概率可以描述为：

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

验证协议满足不可否认性的概率结果约为 0.03125。同理，将 attackNM 设置为 0.5，验证实体 WU 和 CS 所受攻击率不同的情况下，协议满足不可否认性的状态概率。检验结果如图 4 所示，横轴代表实体 WU，CS 间所受攻击率，纵轴代表协议满足不可否认性的状态概率。由检验结果可以得出，协议满足不可否认性的概率随 attackUC 的增大而减小，当 attackUC 的取值为 1 时，协议满足不可否认性的概率为 0；当 attackMC 的取值为 0 时，协议满足不可否认性的概率为 0.0625。

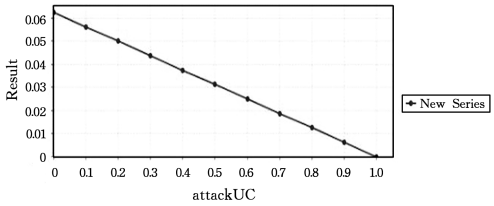

图 4　协议满足不可否认性的概率

Fig. 4　Probability of protocol satisfying non-repudiation characteristics

同理，将 attackUC 设置为 0.5，验证信道 attackNM 与协议满足不可否认性的概率的变化关系，结果如图 5 所示。

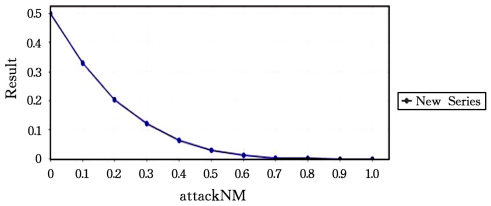

图 5　协议满足不可否认性的概率

Fig. 5　Probability of protocol satisfying non-repudiation characteristics

由图 5 可知，协议满足不可否认性的概率随 attackNM 的增大而减小。当 attackNM 的取值为 0 时，协议满足不可否认性的概率为 0.5；当 attackNM 的取值为 1 时，协议满足不可否认性的概率为 0。

通过同时为 attackUC 和 attackNM 设置不同的值，得到协议满足不可否认性的概率与攻击率的变化关系。

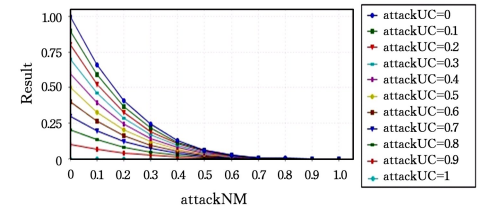

图 6　attackUC 和 attackNM 不同取值下的协议满足不可否认性的概率

Fig. 6　Probability of protocol satisfying non-repudiation characteristics with different attackUC and attackNM values

由检验结果可知，协议满足不可否认性的概率随 attackUC 和 attackNM 取值的增大而减小。

时延性[17]是指消息认证方面都没有出错，但却因为一些其他原因（例如攻击率）而导致一方不能及时达到目的，即云辅助的轻量级无证书认证协议的 WBAN 用户由于一些因素迟迟不能得到云服务器的服务响应，即网络管理者实现了对 WBAN 用户的身份认证，且网络管理者也完成了对云服务器的平台认证，但用户却迟迟没有成功登入云服务器。因此可以将协议时延性描述为：

label "time_ductility"=stopUU & stopNM & stopCS & (sendMessage2 & checkMessage2=1) & (sendMessage4 & checkMessage4=1) & ((sendMessage6 & checkMessage6=2)|(!sendMessage6));

当 attackNM 为固定值 0.5 时，协议满足时延性的状态概率如图 7 所示。

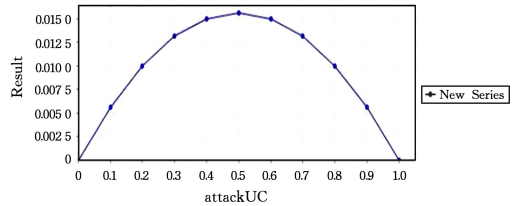

图 7　attackNM 为 0.5 时协议满足时延性的概率

Fig. 7　Probability of protocol satisfaction satisfying time delay when value of attackNM is 0.5

图 7 中横轴代表实体 WU 和 CS 之间消息传递时所受的攻击率，纵轴代表协议满足时延性的状态概率。由检验结果可以得出，只有当 attackUC 的取值为 0 或 1 时，协议满足时延性的概率为 0；当 attackUC 的取值为 0.5 时，协议满足时延性的概率接近最大值，约为 0.015625。在云辅助的轻量级无证书认证协议中，如果协议在运行时受到了很强的攻击，通往 NM 的消息可能不完整，这就相当于没有 NM。因此，本文针对 NM 攻击率进行了验证分析。首先验证当 NM 的攻击率为 1 时，云辅助的轻量级无证书认证协议满足时延性的概率的变化情况，结果如图 8 所示。

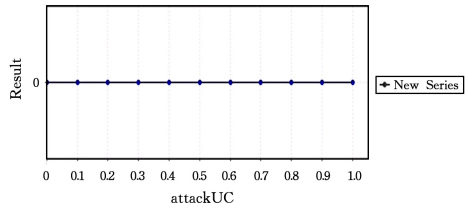

图 8　NM 的攻击率为 1 时协议满足时延性的概率

Fig. 8　Probability of protocol satisfaction satisfying when attack rate of NM is 1

由检验结果可知，当 APS 受到的攻击率为 1 时，整个协议过程将不存在所谓的时延性，移动用户不能成功登入云服务器，宣告失败。由此说明网络管理者起到很重要的作用。

通过同时为 attackUC 和 attackNM 设置不同取值，得到协议满足时延性的概率与攻击率的变化关系。

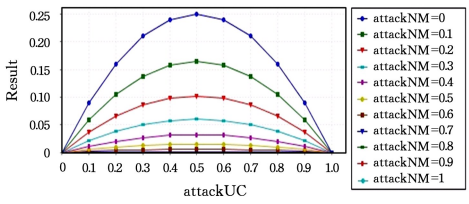

图 9 协议满足时延性的概率与攻击率的关系

Fig. 9 Relationship between probability of protocol satisfying time delay and attack rate

有效性[18]保证了云辅助的轻量级无证书认证协议的 WBAN 用户和云服务器双方在满足协议设计者所设定的通信时的质量，并且 WBAN 用户的请求服务得到了云服务器的响应。可以将协议满足有效性描述为：

label“effective”= stopUU & stopNM & stopCS & (sendMessage5 & checkMessage5 = 1) & (sendMessage6 & checkMessage6 = 1)；

首先验证当 NM 的攻击率为 0 时，即 attackNM = 0 时，攻击率 attackUC 和协议满足有效性的概率变化关系。验证结果如图 10 所示。可以看出，协议满足有效性的概率随 attackUC 的增大而减小。当 attackUC 的取值为 0 时，协议满足有效性的概率为 1；当 attackUC 的取值为 1 时，协议满足有效性的概率为 0。

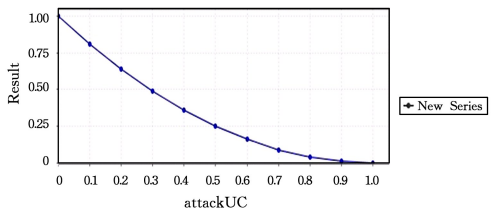

图 10 协议满足有效性的概率

Fig. 10 Probability of protocol satisfying validity

同理，设置 attackUC 的值为 0.5，验证攻击率 attackNM 与协议满足有效性的概率的变化关系，如图 11 所示。

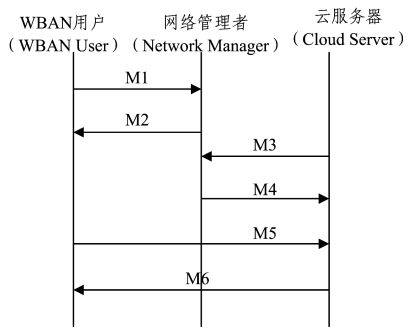

图 11 attackUC 的值为 0.5 时协议满足有效性的概率

Fig. 11 Probability of protocol satisfying validity when value of attackUC is 0.5

由图 11 可知，协议满足有效性的概率随 attackNM 值的增大而减小。当 attackNM 的取值为 0 时，协议满足有效性的概率为 0.25；当 attackNM 的取值为 1 时，协议满足有效性的概率为 0。

通过同时为 attackUC 和 attackNM 设置不同值，得到协议满足有效性的概率与攻击率的变化关系，如图 12 所示。

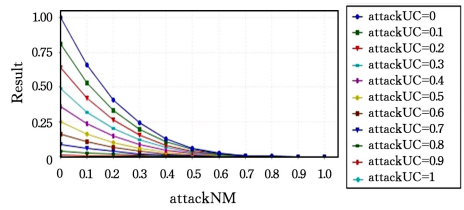

图 12 协议满足有效性的概率

Fig. 12 Probability of protocol satisfying validity

由检验结果可知，协议满足有效性的概率随 attackUC 和 attackNM 取值的增大而减小。

综上所述，云辅助的轻量级无证书认证协议满足重要属性的概率随攻击率 attackUC 和 attackNM 的变化而变化。协议满足不可否认性的概率随 attackUC 和 attackNM 的增大而减小，随 attackUC 的增大先增大后减小，随着 attackNM 的增大而减小。

3.3 协议属性对比

云计算现今仍被认为是一种比较新的技术，云计算技术与传统的 WBANS 相结合，能够存储、处理并实时检测医学数据。早期出现了许多基于客户与服务器之间的无证书认证协议，将 SIP 协议[19]作为对比协议进行有效性对比，结果如图 13 所示。

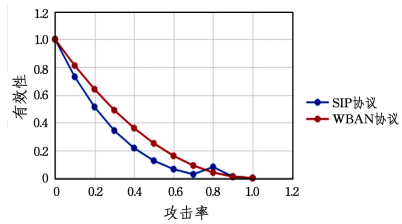

图 13 两个协议的有效性对比图

Fig. 13 Comparison of validity of two protocols

从图 13 中可以明显看出，相同攻击率下，基于云辅助的匿名 WBANs 的轻量级无证书认证协议的有效性总体上优于 SIP 协议的。

从图 14 中可以明显看出，相同攻击率下，基于云辅助的匿名 WBANs 的轻量级无证书认证协议的不可否认性总体上优于 SIP 协议的。

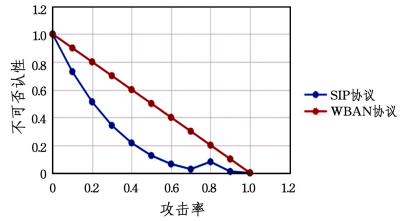

图 14 两个协议的不可否认性对比图

Fig. 14 Non repudiation comparison diagram of two protocols

图 15 表明，相同攻击率下，基于云辅助的匿名 WBANs 的轻量级无证书认证协议的时延性在总体上是劣于 SIP 协议的。由于在协议实体数量方面，匿名 WBANs 的轻量级无证书认证协议比 SIP 协议多一个云服务器实体，因此时延性略差。

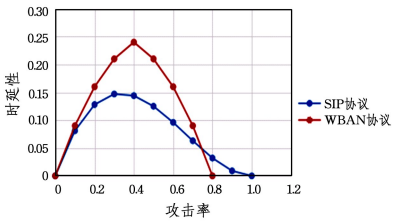

图 15　两个协议的时延性对比图

Fig. 15　Delay comparison diagram of two protocols

结束语　本文将一种基于云辅助的匿名 WBANs 的轻量级无证书认证协议作为研究对象，运用概率模型检测的形式化验证的方法，基于攻击率对云辅助的轻量级无证书认证协议的重要属性进行定量分析，验证了在不同的攻击率条件下，协议满足不可否认性的概率、协议满足时延性的概率和协议满足有效性的概率。同时，将其与 SIP 协议进行了重要属性对比。由检验结果可知，协议各实体间的攻击率对协议的不可否认性、时延性和有效性分别有不同程度的影响，与其他协议比较而言，此协议在有效性和不可否认性方面有着明显优势。因此对相应攻击率进行控制可以提高协议的安全性，进而可以提高医疗服务的质量，以及实时监测和远程医学的基本需求水平，对人类的医疗保健有着很重要的意义。但其仍存在些许不足，即攻击率不好控制，且时延性略差。今后的工作可以从协议的方面进行研究改进，以使其达到更好的效果。

参 考 文 献

[1] ARMBRUST M, FOX A, GRIFFITH R, et al. A view of cloud computing[J]. Communications of the ACM, 2010, 53(4): 50-58.

[2] SMITH D B, MINIUTTI D, LAMAHEWA T A, et al. Propagation Models for Body-Area Networks: A Survey and New Outlook[J]. IEEE Antennas & Propagation Magazine, 2014, 55(5): 97-117.

[3] SABAHI F. Cloud computing security threats and responses [C]// International Conference on Communication Software and Networks. IEEE, 2011: 245-249.

[4] CHEN T, KWIATKOWSKA M, PARKER D, et al. Verifying Team Formation Protocols with Probabilistic Model Checking [M]// Computational Logic in Multi-Agent Systems. Springer Berlin Heidelberg, 2011: 190-207.

[5] LAPLANTE S, LASSAIGNE R, MAGNIEZ F, et al. Probabilistic abstraction for model checking: an approach based on property testing[J]. Proceedings-Symposium on Logic in Computer Science, 2002, 8(4): 30-39.

[6] HEATH J, KWIATKOWSKA M, NORMAN G, et al. Probabilistic Model Checking of Complex Biological Pathways[M]// Computational Methods in Systems Biology. Springer Berlin Heidelberg, 2006: 32-47.

[7] FENG B, MA X, GUO C, et al. An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing [J]. IEEE Access, 2017, 4(99): 7899-7911.

[8] YANG B, FENG D G, QIN Y, et al. Secure Access Scheme of Cloud Services for Trusted Mobile Terminals using TrustZone [J]. Journal of Software, 2016, 27(6): 1366-1383. (in Chinese)
杨波，冯登国，秦宇，等. 基于 TrustZone 的可信移动终端云服务安全接入方案[J]. 软件学报，2016，27(6)：1366-1383.

[9] WU L B, ZHANG Y B, HE D B. Identity based double server ciphertext equivalence decision protocol in cloud computing[J]. Computer Research And Development, 2017, 54(10): 2232-2243. (in Chinese)
吴黎兵，张宇波，何德彪. 云计算中基于身份的双服务器密文等值判定协议[J]. 计算机研究与发展，2017，54(10)：2232-2243.

[10] SHEN J, GUI Z, JI S, et al. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks[J]. Journal of Network & Computer Applications, 2018, 106: 117-123.

[11] KWIATKOWSKA M, NORMAN G, PARKER D. Advances and challenges of probabilistic model checking[C]// Communication, Control, and Computing. IEEE, 2010: 1691-1698.

[12] SHARIR M, PNUELI A, HART S. Verification of probabilistic programs[M]. Society for Industrial and Applied Mathematics, 1984.

[13] KWIATKOWSKA M, NORMAN G, PARKER D. PRISM 4.0: Verification of Probabilistic Real-Time Systems[J]. Lecture Notes in Computer Science, 2011, 6806: 585-591.

[14] LIU L, HASAN O, TAHAR S. Formal Reasoning About Finite-State Discrete-Time Markov Chains in HOL[J]. Journal of Computer Science & Technology, 2013, 28(2): 217-231.

[15] BALTAZAR P, MATEUS P, NAGARAJAN R, et al. Exogenous Probabilistic Computation Tree Logic[J]. Electronic Notes in Theoretical Computer Science, 2007, 190(3): 95-110.

[16] ROSTAMI M, BAGHERI E, LOTFI M. Cooperating the web services as distributed to create a Non- Repudiation service[J]. International Proceedings of Economics Development & Research, 2007, 4526: 9-19.

[17] WANG J, WANG Z, DING S, et al. Refined Jensen-Based Multiple Integral Inequality and Its Application to Stability of Time-Delay Systems[J]. IEEE/CAA Journal of Automatica Sinica, 2018, 5(3): 758-764.

[18] KREMER S. Formal Analysis of Optimistic Fair Exchange Protocols[J]. Journal of Software, 2003, 2004(3): 509-521.

[19] WU L, ZHANG Y, WANG F. A new provably secure authentication and key agreement protocol for SIP using ECC[J]. Computer Standards & Interfaces, 2009, 31(2): 286-291.