

基于信任评估的卫星物联网终端认证方法

田敏求^{1,2,3}, 李凤华^{1,2,3}, 李子孚^{1,3}, 郭超^{1,3,4}

(1.中国科学院信息工程研究所, 北京 100085; 2.中国科学院大学网络空间安全学院, 北京 100049;
3.网络空间安全防御重点实验室, 北京 100085; 4.北京电子科技学院电子与通信工程系, 北京 100070)

摘要: 卫星物联网利用卫星通信网络、星载及地面多种类型终端设备, 能够实现空天地一体化的人、物连接和信息交互, 具有空中无界、地面无障的优势, 也有大尺度覆盖、链路高度开放、拓扑动态变化、终端资源受限、通信时延长等特点。为了实现卫星物联网资源的安全高效利用, 提出了基于信任评估的卫星物联网终端认证方法, 通过对终端设备进行信任评估来优化认证策略。针对曾经强认证的终端短时间内再次认证, 和经由强认证节点授信两种情形, 提出了卫星物联网终端信任评估机制, 按照直接信任和间接信任刻画了动态调整的信任度量和评估模型, 设计了基于信任评估的卫星物联网接入认证协议, 根据设备信任度采用相匹配的认证机制, 使高信任度设备的后续认证流程得以简化, 实现了在同一认证策略框架下为不同终端设备提供差异化的认证服务。使用非形式化方法和 Tamarin 形式化工具对协议安全性进行全面分析, 通过实验验证协议的有效性, 可降低总体认证开销, 且可利用信任简化认证流程。

关键词: 卫星物联网; 接入认证; 信任评估; 形式化验证

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024051

Satellite IoT terminal authentication method based on trust evaluation

TIAN Minqiu^{1,2,3}, LI Fenghua^{1,2,3}, LI Zifu^{1,3}, GUO Chao^{1,3,4}

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China

2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

3. Key Laboratory of Cyberspace Security Defense, Beijing 100085, China

4. Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: Satellite internet of things (satellite IoT) has been utilized to achieve the integration of space-ground, human-thing connection, and information interaction through the satellite communication network and various types of spaceborne and ground terminal devices. It possesses advantages that are boundless in air and unobstructed on ground, as well as characteristics such as large-scale coverage, highly open links, dynamically changing topolo-

收稿日期: 2024-03-10; 修回日期: 2024-07-18

通信作者: 郭超, guo99chao@163.com

基金项目: 国家自然科学基金 (U23B2024, 62202463)

Foundation Item: The National Natural Science Foundation of China (U23B2024, 62202463)

引用格式: 田敏求, 李凤华, 李子孚, 等. 基于信任评估的卫星物联网终端认证方法[J]. 网络与信息安全学报, 2024, 10(4): 37-48.

Citation Format: TIAN M Q, LI F H, LI Z F, et al. Satellite IoT terminal authentication method based on trust evaluation[J]. Chinese Journal of Network and Information Security, 2024, 10(4): 37-48.

gies, limited terminal resources, and long communication latency. In order to achieve the safe and efficient utilization of satellite IoT resources, a trust evaluation-based terminal authentication method for satellite IoT was proposed, which could optimize the authentication strategy by evaluating the trust of terminal devices. A trust evaluation mechanism for satellite IoT terminals was proposed for two scenarios: terminals that had recently undergone strong authentication and had been granted credit by strongly authenticated nodes. A dynamically adjusted trust measurement and evaluation model was characterized based on direct trust and indirect trust. Secondly, a trust evaluation-based access authentication protocol for satellite IoT was designed, which adopted a matching authentication mechanism according to the trust degree of the device. This allowed for the simplification of the subsequent authentication process for high-trust devices and provided differential authentication services for different terminal devices under the same authentication strategy framework. The security of the protocol was comprehensively analyzed using non-formal methods and Tamarin formal tools, and the effectiveness of the protocol was verified by experiments. The protocol was shown to be capable of reducing the overall authentication overhead and simplifying the authentication process with trust.

Keywords: satellite IoT, access authentication, trust evaluation, formal verification

0 引言

卫星通信网络是一种天地一体化信息网络,通过卫星等航天技术将地球上的各个区域连接起来,实现了全球范围内的通信覆盖^[1]。在万物互联时代,物联网终端广泛应用于气候感知、智能家居设备、工业控制等各个领域^[2]。采用卫星通信网络技术连接遍布全球的物联网终端,提供空地立体、广域无缝覆盖的通信和管理能力,形成了卫星物联网^[3]。卫星物联网增强了物联网的网络层,将卫星通信延伸至物联网终端,因而同时具备卫星通信网络和物联网的特点。在卫星物联网资源受限的条件下,为了实现网络资源的安全高效利用,有效防止非法接入和恶意攻击,设计轻量级、多样化的安全认证机制对于卫星物联网的安全接入和功能保障具有重要意义^[4]。

卫星物联网中卫星、地面站、用户终端等各种实体之间信任关系的度量由各自的属性和行为决定。考虑这些影响信任的因素通常处于动态变化的状态,不同信任关系之间有相关性^[5]。同时卫星物联网中存在不可信终端,发现并量化这些终端的信任度,成为设计轻量级、多样化安全认证方案的关键问题。本文的研究动机是结合卫星物联网业务特点,将与信任有关的信息进行转化,给出信任度量和评估模型,信任评估的动态特性确保及时反映当前各种设备类型的信任度情况,并可根据不同需求进行定制和扩展。本文的主要贡献如下。

1) 针对曾经强认证的终端短时间内再次认证,和经由强认证节点授信两种情形,按照直接信任和间接信任刻画了信任度量和评估模型,给出了信任度和信任度阈值计算方法。

2) 采用哈希链和 SM2 数字签名技术,设计了基于信任评估的接入认证协议,根据设备信任度采用相匹配的认证机制,使高信任度设备的后续认证流程得以简化。

3) 对上述协议进行安全性分析,并通过实验验证协议的有效性,能够降低总体认证开销的同时,实现在同一认证策略框架下为不同终端设备提供差异化的认证服务。

1 相关工作

随着卫星通信技术的兴起,关于卫星在物联网中的应用研究近年来备受关注,而安全认证协议对保障卫星物联网安全至关重要。Xue 等^[6]确定了卫星物联网安全认证协议的一些基本安全要求,提出了基于椭圆曲线密码的高效认证协议,实现了对终端和卫星的双向认证。Ma 等^[7]提出了基于格密码的卫星物联网接入认证方案,目标卫星节点通过验证单签名和辅助信息对物联网终端进行认证。

终端卫星直连认证方案可以显著减少卫星与地面之间的交互,有效降低认证时延。Meng 等^[8]设计了短时延的空间信息网络快速接入认证方案,通过代理签名确保授权的卫星才能从网关获得认证用户的权限,有效降低卫星遭劫持攻击

的风险。Xue等^[9]基于椭圆曲线密码提出了终端卫星直连认证模型，有效降低认证时延且避免了地面控制中心单点失效。虽然文献[8-9]有效实现了直连认证，但不具备匿名性、前向安全性等属性，且涉及复杂的双线性对计算开销。为了实现匿名性和监管功能，Yang等^[10]基于群签名提出了快速漫游认证方案，不仅实现了直连匿名认证，还有效提供了追责和撤销机制，但该方案仍涉及双线性对运算和大量点乘运算，难以实现高性能、低带宽的目标。曹进等^[11]针对星地、星间和层间场景提出了适用于双层卫星通信网络的完整认证协议，该认证协议对双层卫星通信网络进行层次化管理，细化了认证管理体系，并使用了群密钥保障卫星身份信息等信息不被非法卫星获取，在增强认证安全的同时，也增加了带宽开销。

国内外学者在卫星物联网的安全认证领域已经取得一定进展，但现有的认证机制设计成型后难以动态调整，不能很好地解决通信效率低、业务连续性不佳等问题。从认证策略角度看，存在灵活性上的局限，难以满足差异化的认证需求。

2 预备知识

2.1 网络信任模型

网络信任模型根据信任来源，可以分为直接信任和间接信任，所依赖的授信基础主要包括业务应用信息流、基础通信网络、终端人机交互等方面。单纯由通信主体独立产生的信任度量称为直接信任。这种独立产生的信任度量往往基于以往信任客体（被授信方）的通信行为、通信能力等特征进行评估。这种基于通信行为的评估会产生一定的波动，通常需要额外的知识信息进行校正。先验的知识也可作为授信的依据，比如用户的归属、通信能力和配置文件。另外，用户提供知识的深度、细节程度和具体内容同样可帮助体现它们的真实性和意图。直接信任模型下，信任的度量通过相互评级实现，这种评级依赖于环境信息或者由被授信者提供的信息，因而会受到双方所处的网络环境的影响，即在一种网络条件下的正常行为，在另一种网络条件下很可能是异常的，所以需要针对交互环境设计相应的评估机制。

对于一个从未交互过的节点，很难建立直接信任，这就需要中间方进行间接的授信。间接信

任中，任何两个节点之间都需要有一个或者多个中间节点，形成有向路径——每个节点为它后面的节点提供信任值，形成一个可靠的信任链，用以进行信任传递。在实现信任值传播后，可以对每个路径的信任值进行合并，这时需要引入信任聚合的方法来衡量哪些路径更加可信，并将不同的信任值相结合起来计算信任度。间接信任需要注意信任值传播路径的拓扑和尺寸。当信任路径上存在环或者过多的路径时，如何聚合、分离重复的路径将使信任度的计算变得非常复杂。同时，随着信任值传播路径的增加，信任度随之衰减。

2.2 贝叶斯预测模型

贝叶斯预测模型（Bayesian forecasting model）是一种基于概率理论的统计方法，核心是利用贝叶斯定理来合并先验知识和新的观测数据，从而更新对某事件或参数的概率估计。这种方法在决策理论、统计推断和预测等多个领域有广泛应用。通过这种方法，可以将先验概率与似然性相结合起来，生成后验概率。

在通信网络中，贝叶斯模型可以有效地预测和处理不确定性信息，尤其是在面对大规模数据和复杂网络环境时。例如，在设备的信任度计算中，可以通过计算一定周期内有效数据包比例来预测未来相似周期内数据包的有效性，从而对设备的信任度进行动态调整。总体而言，贝叶斯预测模型提供了一种有效的方式来处理含有不确定性的复杂数据，在多个领域中得到了实际应用，尤其是在需要进行精确分类和预测的场合。

3 系统概述

3.1 系统模型

卫星物联网系统模型如图1所示，按照卫星物联网系统架构，分为应用段、地面段和空间段3个部分，各部分功能和相互关系的具体描述如下。

（1）应用段

应用段由部署在不同位置的各种卫星物联网终端设备组成，这些设备通常配备了卫星通信模块，能够与卫星进行数据和指令的收发。应用段的卫星物联网终端包括海量静态传感设备、大型数据传输设备、高速移动终端设备3种类型。海量静态传感设备计算能力较弱，内存空间小，一般为单向发送数据，因此海量静态传感设备可认

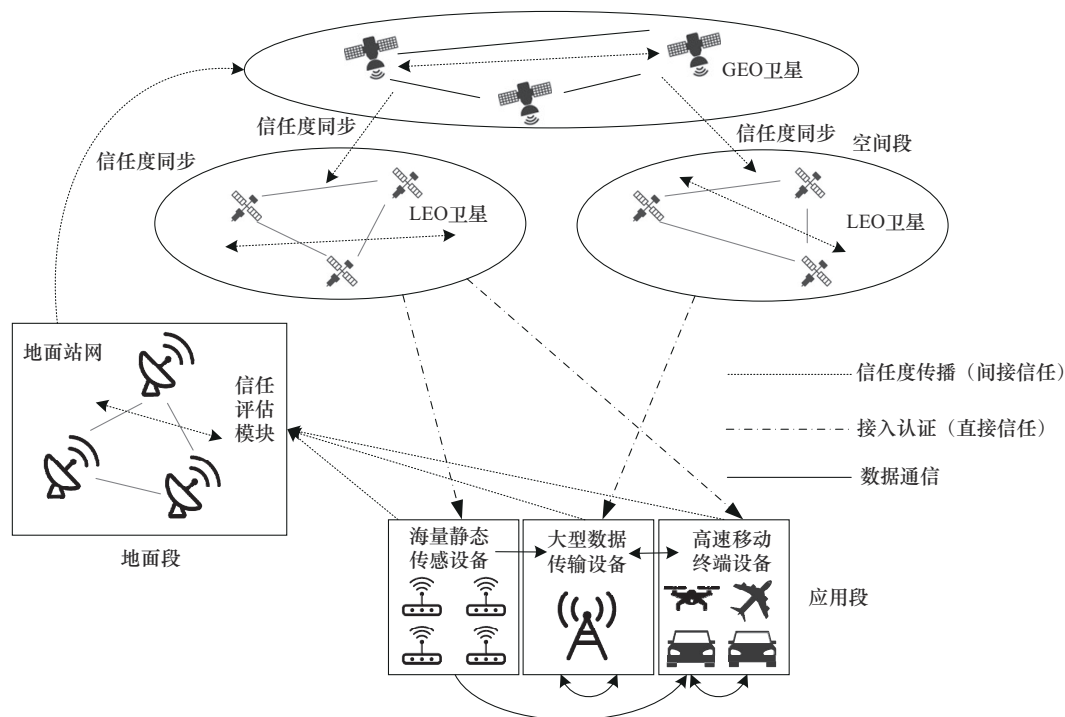


图1 卫星物联网系统模型

Figure 1 Satellite IoT system model

为只与大型数据传输设备、高速移动终端设备进行单向数据通信，该类设备内部之间不会进行数据通信。大型数据传输设备具备较强大的计算、存储和通信能力，在该类设备内部之间，以及与高速移动终端设备之间都可以进行双向数据通信，如接收传感器设备的传感信息、不同地面基站之间的相互访问和数据传输、向无人机或车辆等高速移动终端提供数据信息服务等。高速移动终端设备与大型数据传输设备类似，同样可以进行双向数据通信，区别是大型数据传输设备由于位置固定，数据通信多为长时间稳定连接，而高速移动终端设备的数据通信则往往需要不断切换，可能存在较多断续连接的情况。

(2) 地面段

地面段主要是信关站等构成的地面站网。地面站被视作经过强认证的可信节点，主要用于建立间接信任。地面站扮演着信任度计算机构角色，每个地面站都安装信任评估模块，负责存储、计算和更新不同类型的各个设备的信任度，并不断在地面站网内同步，同时向地球同步轨道（geostationary earth orbit, GEO）卫星传递信任度信息并持续更新，以有效管理和优化卫星物联

网的运转，提升系统的整体性能和可靠性。

(3) 空间段

空间段包括 GEO 卫星和低地球轨道（low earth orbit, LEO）卫星。GEO 卫星相较 LEO 卫星处于距离地球更远的位置，可以同时覆盖多颗 LEO 卫星，因此 LEO 卫星和 GEO 卫星根据它们的位置被分成不同群组，每个群组有 1 颗 GEO 卫星和若干颗 LEO 卫星。GEO 卫星主要负责持续接收地面站网提供的最新信任度信息，并将其同步给所覆盖的本群组内的所有 LEO 卫星。LEO 卫星接收到信任度信息后，针对曾经强认证的终端短时间内再次认证，和经由强认证节点授信两种情形，借助信任度信息对其所覆盖的地面卫星物联网终端设备实施灵活的认证机制。本文中将 LEO 卫星视为完全可信的，所以在认证协议设计上只涉及 LEO 卫星对终端设备的单向认证。

3.2 威胁模型及安全假设

在卫星物联网系统模型中，实体间安全交互方案设计的前提是对系统的威胁模型进行分析，在此先给出卫星、地面站和卫星物联网终端的安全假设。

1) LEO 卫星和 GEO 卫星被认为是完全可信

的,会如实地进行通信和传输,也会如实地存储和更新各个卫星物联网终端的信任度。

2) 地面站也被认为是完全可信的,会如实地记录卫星物联网终端产生的访问和通信行为,对这些行为进行正确的信任度计算和存储,并将信任度信息诚实地发送给GEO卫星。

3) 卫星物联网终端是半可信的,不会主动作恶,如果存在恶意节点或者被劫持,则会发生静默、传输错误数据、恶意访问等行为。

4) 安全认证不涉及终端的接入网络制式,也不涉及物理层的信道及链路层协议,地面站网之后的地面网络(如电信网、互联网)不被纳入安全认证考虑范围。

基于上述安全假设,在LEO卫星对不同类型终端设备进行认证时,敌手可以通过实施重放攻击、篡改攻击、劫持攻击等,造成认证过程失败或恶意设备通过认证等后果。对此需要实现的安全目标如下。

(1) 信任评估的准确性

确保通过地面站网的信任评估模块计算得到的信任度和信任度阈值能够如实反映出不同周期单个设备和每一设备类型的信任情况。

(2) 数据完整性

敌手可能篡改消息和实施恶意攻击,导致通信数据被破坏,所以应保证发送数据与接收数据是一致的。

(3) 不可伪造性

确保接收到的数据由合法实体发送,确保发送数据的实体确实具有所声称的身份,即保证参与交互的实体是真实的,不会被敌手冒充。

(4) 抗重放攻击

防止敌手发送一个LEO卫星已经接收过的消息来达到欺骗LEO卫星通过认证的目的。

(5) 不可抵赖性

LEO卫星对不同类型终端设备进行认证时,确保LEO卫星可以防止不同类型终端设备的抵赖行为。

4 方案设计

针对增强现有认证机制灵活性和卫星物联网差异化的安全认证需求,本文设计卫星物联网终端信任评估机制,考虑曾经强认证的终端短时间

内再次认证,和经由强认证节点授信两种情形,按照直接信任和间接信任刻画动态调整的信任度和评估模型。在此基础上,采用哈希链和SM2数字签名技术,设计基于信任评估的接入认证协议,根据设备信任度采用相匹配的认证机制,实现在同一认证策略框架下为不同终端设备提供差异化的认证服务。

4.1 信任评估机制

本文提出的卫星物联网终端信任评估机制,旨在针对曾经强认证的终端短时间内再次认证,和经由强认证节点授信,利用信任简化后续认证流程。曾经强认证的终端短时间内再次认证,可被认为之前建立了直接信任,信任度随着时间推移而衰减;经由强认证节点授信可被认为是间接信任。本文取一个通信周期内接收到的有效数据包与所有数据包的数量关系来衡量通信满意度 S ,基于贝叶斯预测模型计算不同类型设备的信任度。考虑直接信任的建立有赖于之前要经过强认证,如果未经过强认证,只进行了简化认证,则通过间接信任来度量,由此将信任评估机制分为直接信任和间接信任两种计算方法。令 $t_{n,i}$ 代表设备 i 在第 n 个通信周期时的信任度($t_{n,i} \in [0,1]$),初始状态下所有设备信任度 $t_{0,i} = 0$ 。

4.1.1 直接信任

曾经强认证的终端短时间内再次认证的情形适用于直接信任评估。由于之前经过强认证, $t_{n,i}$ 的计算方法较为简单。如果上一次认证为强认证,可以认为通过强认证的时刻 $t_{n,i} = 1$,此后信任度随着时间的推移而衰减,可利用连续的指数衰减形式进行描述^[12]。令每个通信周期的时间长度为 τ ,距上一次通过强认证已经过了 m 个通信周期,则 $t_{n,i}$ 可表示为

$$t_{n,i} = e^{-\omega m \tau} \quad (1)$$

其中, $\omega \in [0,1]$,用于表示信任度随着时间推移而衰减的预设参数。式(1)对于海量静态传感设备、大型数据传输设备和高速移动终端设备3种设备类型都是适用的。令 $t_{n,X}$ 代表设备类型 X 的信任度阈值,由于在直接认证条件下每个终端的信任度彼此是独立的, $t_{n,X}$ 的值要依靠历史经验来确定。

4.1.2 间接信任

经由强认证节点授信的情形适用于间接信任

评估, 如果上一次认证为简化认证, 则只能依靠地面站作为经过强认证的节点给出终端设备的信任度。因为之前未经过强认证, 间接信任的建立较复杂。为了度量信任, 考虑基于数据接收方对数据发送方的评价来刻画数据发送方的信任度。具体而言, 设计通信满意度的指标 S , 然后基于通信满意度刻画不同类型的卫星物联网终端设备的信任度并进行动态调整。通信满意度指标 S 由数据接收方给出, 每一次通信行为后, 接收方都会向就近的地面站反馈该次通信的满意度, 地面站信任评估模块基于通信满意度来综合计算数据发送方设备的信任度 $t_{n,i}$ 。同直接信任类似, 每一种设备类型会有一个信任度阈值 $t_{n,X}$, 由于间接信任与各个设备之间的通信行为和彼此信任程度有关, 该信任度阈值由该类型所有设备的信任度共同决定。这里假设地面站向 GEO 卫星传输设备信任度信息、GEO 卫星向 LEO 卫星同步设备信任度信息的时间均远小于信任度的更新周期, 因此可以认为在安全认证的过程中, 单个设备的信任度和这一设备类型的信任度阈值不会发生改变。同时, 各个设备对信任评估的标准相同, 即针对同一次通信行为, 不同设备的评估结果应当相同, 也不存在为了自身利益进行合谋来提高自身信任度的情况。针对 3 种设备类型的信任度评估机制如下。

(1) 海量静态传感设备类型

海量静态传感 (以下用 Type-I-User 代指) 设备由于只发送数据, 不存在数据的接收, 所以不涉及通信满意度的反馈, 同时该类型设备的数据发送以通信时间短、单次通信数据量小、通信频率不固定为特点。

某个 Type-I-User 设备 i 在第 n 个通信周期时, 其信任度 $t_{n,i}$ 取决于两方面因素: 一是第 $n-1$ 个通信周期时的历史信任度 $t_{n-1,i}$, 二是本次通信时接收方对其给出的通信满意度。设接收方为其他类型设备 j , 其对设备 i 发送来的数据的通信满意度为 $S_{n,i} \in [0,1]$, 则第 n 次通信时设备 i 的信任度 $t_{n,i}$ 可表示为:

$$t_{n,i} = \alpha \cdot \delta \cdot S_{n,i} + (1 - \alpha) \cdot t_{n-1,i} \quad (2)$$

其中, $\alpha, \delta \in [0,1]$ 。 α 为预设参数, 用于调节当次满意度和历史信任度对 $t_{n,i}$ 影响的比值。 δ 为接收

方设备 j 的信任度参数, 其值为:

$$\delta = \begin{cases} \frac{t_{n,X} - t_{n,j}}{t_{n,X}}, & t_{n,X} > t_{n,j} \\ 1, & t_{n,X} \leq t_{n,j} \end{cases} \quad (3)$$

其中, $t_{n,X}$ 是设备 j 所属 X 设备类型在第 n 次通信时的信任度阈值, $t_{n,j}$ 为设备 j 在第 n 个通信周期时的信任度。换言之, 如果设备 j 的信任度高于其所属设备类型的信任度阈值, 则 δ 取值为 1, 否则设备 j 给出的通信满意度应有一定比例的折扣, 这是设备 j 自身信任度不足导致的。

由于该类型设备通信行为简单, 时间短且不涉及对其他类型设备的满意度反馈, Type-I-User 设备类型的信任度阈值 $t_{n,I}$ 为当前通信周期内所有该类型设备的信任度平均值, 即 $t_{n,I} = \bar{t}_{n,i}$ 。

(2) 大型数据传输设备类型

大型数据传输 (以下用 Type-II-User 代指) 设备可在该类型设备内部, 以及与其他类型设备之间进行双向的数据传输。首先, 该类型设备不涉及主动与 Type-I-User 设备进行通信, 而只是被动单向地接收 Type-I-User 设备发来的数据, 期间自身信任度不会发生变化, 无须考虑此类通信。其次, 该类型设备与同类型其他设备或高速移动终端 (以下用 Type-III-User 代指) 设备需要建立较长时间通信, 期间存在多数据包传输情况。传输的数据包中包括格式合法且数据正确的数据包, 称为有效数据包; 也包括被恶意节点篡改或在传输过程中损坏的数据包, 称为无效数据包。因此, 用一个通信周期内该类型设备发送的有效数据包与所有数据包的数量关系来描述接收方对该类型设备的通信满意度。

在此部分中, 借鉴文献[13]中计算自治系统信任度的相关方法, 将设备是否接收到有效数据包看成是二项事件, 则设备在某个时间周期内收到的有效数据包数服从二项分布。假设某个 Type-II-User 设备 i 在第 n 个通信周期内与其他设备进行了长时间通信, 期间共发送了 N_i 个数据包, 其中有 r_i 个数据包是有效的。根据贝叶斯预测模型^[14], 预测设备 i 未来发送的 K_i 个数据包中有 z_i 个是有效的, 那么在 r_i 的条件下得到 z_i 的条件概率 $P(z_i | r_i)$ 为:

$$P(z_i|r_i) = C_{K_i}^{z_i} \cdot \frac{\Gamma(N_i + 2) \cdot \Gamma(r_i + z_i + 1) \cdot \Gamma(N_i - (r_i + z_i) + K_i + 1)}{\Gamma(r_i + 1) \cdot \Gamma(N_i - r_i + 1) \cdot \Gamma(N_i + K_i + 2)} \quad (4)$$

其中, $C_{K_i}^{z_i}$ 表示组合数, 即从 K_i 数据包中选出 z_i 个数据包有多少种选法。

设 $z'_i = \left\{ z_i \mid \max_z \{p(z_i | r_i)\} \right\}$ 为最有可能的 z_i 值。则最终该周期的满意度 $S_{n,i} = \frac{r_i + z'_i + 1}{N_i + K_i + 2}$, 该周期设备 i 的信任度为:

$$t_{n,i} = \alpha \cdot \delta \cdot S_{n,i} + (1 - \alpha) \cdot t_{n-1,i} \quad (5)$$

其中, $\alpha, \delta \in [0,1]$, 其含义与表示海量静态传感设备信任度的式(2)中的相同。

Type-II-User 设备类型的信任度阈值计算方

$$P(z_1|r_1) = C_{K_1}^{z_1} \cdot \frac{\Gamma(N_1 + 2) \cdot \Gamma(r_1 + z_1 + 1) \cdot \Gamma(N_1 - (r_1 + z_1) + K_1 + 1)}{\Gamma(r_1 + 1) \cdot \Gamma(N_1 - r_1 + 1) \cdot \Gamma(N_1 + K_1 + 2)} \quad (6)$$

设 $z'_1 = \left\{ z_1 \mid \max_z \{p(z_1 | r_1)\} \right\}$ 为最有可能的 z_1 值, 则最终该周期内所有 Type-II-User 设备之间的满意度 $S_{\theta,II-II} = \frac{r_1 + z'_1 + 1}{N_1 + K_1 + 2}$ 。

同时, 在 θ 时间周期内所有 Type-II-User 设

$$P(z_2|r_2) = C_{K_2}^{z_2} \cdot \frac{\Gamma(N_2 + 2) \cdot \Gamma(r_2 + z_2 + 1) \cdot \Gamma(N_2 - (r_2 + z_2) + K_2 + 1)}{\Gamma(r_2 + 1) \cdot \Gamma(N_2 - r_2 + 1) \cdot \Gamma(N_2 + K_2 + 2)} \quad (7)$$

设 $z'_2 = \left\{ z_2 \mid \max_z \{p(z_2 | r_2)\} \right\}$ 为最有可能的 z_2 值, 则最终该周期内所有 Type-III-User 设备对 Type-II-User 设备的通信满意度 $S_{\theta,III-II} = \frac{r_2 + z'_2 + 1}{N_2 + K_2 + 2}$ 。

综上, Type-II-User 设备类型的信任度阈值为:

$$t_{\theta,II} = \beta \cdot S_{\theta,II-II} + \gamma \cdot t_{\theta-1,III} \cdot S_{\theta,III-II} + (1 - \beta - \gamma) \cdot t_{\theta-1,II} \quad (8)$$

其中, $\beta, \gamma \in [0,1]$ 且 $0 \leq \beta + \gamma \leq 1$ 。 β 和 γ 为预设参数, 用于调节各部分因素对 $t_{\theta,II}$ 影响的比值。 $t_{\theta-1,III}$ 表示上一周期 Type-III-User 设备类型的信任度阈值, $S_{\theta,II-II}$ 表示对当前周期 Type-II-User 设备类型内部传输行为的通信满意度, $S_{\theta,III-II}$ 表示对当前周期向 Type-III-User 设备类型进行传输行为所有 Type-III-User 设备给出的通信满意度。

(3) 高速移动终端设备类型

高速移动终端设备与大型数据传输设备类

法与上述计算方法类似, 同样取决于在本类型设备内部及与其他类型设备之间的通信满意度, 以及历史信任度阈值两方面因素。考虑该类型设备与不同设备通信的开始时间和持续时间均不相同, 所以选取一个固定的时间周期 θ 。设 θ 时间周期内所有 Type-II-User 设备向同类型的设备共发送了 N_1 个数据包, 其中有 r_1 个数据包是有效的。同样地, 预测该类型所有设备未来发送的 K_1 个数据包中有 z_1 个是有效的, 那么在 r_1 的条件下得到 z_1 的条件概率 $P(z_1|r_1)$ 为:

备向 Type-III-User 设备共发送了 N_2 个数据包, 其中有 r_2 个数据包是有效的, 那么预测该类型所有设备未来发送的 K_2 个数据包中有 z_2 个是有效的, 在 r_2 的条件下得到 z_2 的条件概率 $P(z_2|r_2)$ 为:

似, 也可以在该类型设备内部, 以及与其他类型设备之间进行双向的数据传输。因此, Type-III-User 设备与 Type-II-User 设备的通信满意度和信任度计算方法相同, 如式(5)所示。

类似地, 在 θ 时间周期内所有 Type-III-User

设备之间的通信满意度为 $S_{\theta,III-III} = \frac{r_2 + z'_2 + 1}{N_2 + K_2 + 2}$ 。

Type-III-User 设备类型的信任度阈值为:

$$t_{\theta,III} = \beta \cdot S_{\theta,III-III} + \gamma \cdot t_{\theta-1,II} \cdot S_{\theta,II-III} + (1 - \beta - \gamma) \cdot t_{\theta-1,III} \quad (9)$$

其中, $\beta, \gamma \in [0,1]$ 且 $0 \leq \beta + \gamma \leq 1$ 。 β 和 γ 为预设参数, 含义同前。 $t_{\theta-1,II}$ 表示上一周期 Type-II-User 设备类型的信任度阈值, $S_{\theta,III-III}$ 表示对当前周期 Type-III-User 设备类型内部传输行为的通信满意度, $S_{\theta,II-III}$ 表示对当前周期向 Type-II-User 设备类型进行传输行为, 所有 Type-II-User 设备给出的通信满意度。

4.2 基于信任评估的接入认证协议

本文基于哈希链的单向多层级认证和 SM2 数字签名技术, 设计基于信任评估的卫星物联网差异化接入认证 (trust evaluation-based differential authentication, TRE-DA) 协议, 该协议用到的符号定义及描述如表 1 所示。

表 1 符号定义及描述

Table 1 Definitions and descriptions of notations

符号	描述
devID_i	设备 i 的编号
$(\text{PK}_i, \text{SK}_i)$	SM2 算法公私钥对
Hash	安全哈希函数
h_{i_0}	安全哈希函数的初始值
n	当前通信周期
m	距上一次通过强认证过的通信周期
τ	每个通信周期的时间长度
$t_{0,i}$	设备 i 的初始信任度
$t_{n,i}$	第 n 个通信周期时设备 i 的信任度
$t_{n-1,i}$	第 $n-1$ 个通信周期, 设备 i 的历史信任度
$S_{n,i}$	接收方对设备 i 给出的通信满意度
$t_{n,X}$	第 n 个通信周期时设备类型 X 的信任度阈值
T_n, T'_n	时间戳
Request _{i}	认证申请
r	挑战值(随机数)
σ_r	对时间戳 T'_n 和挑战值 r 生成的数字签名

在 TRE-DA 协议中, 初始化后由于 $t_{0,i} = 0$, 所有设备终端在首次认证时都会被强制执行强认证机制。此后的每次认证都以信任评估机制为基础, 如果上一次认证是强认证, 则使用直接信任的方法计算 $t_{n,i}$, 如果上一次认证是简化认证, 则使用间接信任的方法计算 $t_{n,i}$, 然后按照每个终端设备的信任度 $t_{n,i}$ 是否高于信任度阈值 $t_{n,X}$, 将其动态地分为高信任度和低信任度设备。每次申请认证时, 所有设备终端都会先尝试采用基于哈希链的简化认证机制, 对于高信任度设备, 简化认证通过则直接进入数据传输阶段; 对于低信任度设备, 即使简化认证通过, 仍需要进一步执行基于数字签

名的挑战一应答的强认证机制。TRE-DA 协议认证流程如图 2 所示。

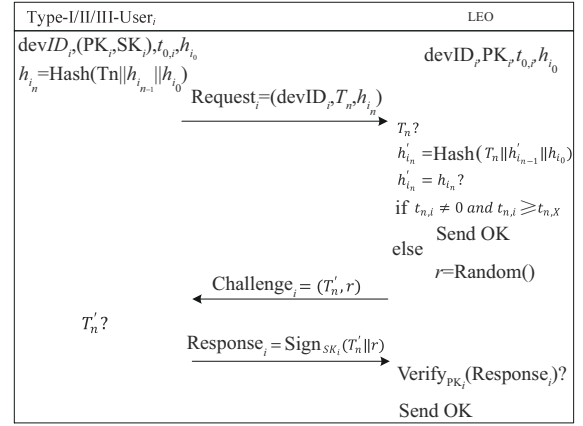


图 2 TRE-DA 协议认证流程

Figure 2 Authentication phase of TRE-DA protocol

1) 初始化

输入安全参数 λ , 由地面站为设备 i 生成其设备编号 devID_i , 获得当前通信时间戳 T_n , 设备初始信任度 $t_{0,i} = 0$ 。随机选取大素数 q , 确定系统参数 $(E, a, b, q, \mathbb{G}, n, G, \mathcal{H}_v, \mathcal{H})$, 其中 $E: y^2 = x^3 + ax + b \pmod{q}$ ($a, b \in \mathbb{Z}_q^*$) 为非奇异椭圆曲线, $\mathbb{G}$ 为在 E (包含无穷远点) 中选取的素数 n 阶循环群, $G \in \mathbb{G}$ 为生成元, $\mathcal{H}_v: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^v$ 为哈希函数。随机选取 $d \in \mathbb{Z}_n^*$, 计算 $P = dG$, 生成 SM2 签名算法公私钥对 $(\text{PK}_i, \text{SK}_i) = (P, d)$ 。 $\mathcal{H}$ 是一个安全哈希函数 (可实例化为 SM3 密码杂凑算法) $\text{Hash}: \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_n^*$ 及其初始值 h_{i_0} 。 devID_i 、 PK_i 、 $t_{0,i}$ 和 h_{i_0} 通过安全信道传递给 LEO 卫星, 其中, h_{i_0} 由双方秘密保存, 用于后续认证。

(2) 信任度评估

输入设备编号 devID_i 、每个通信周期的时间长度 τ 、距上一次强认证已经过的通信周期个数 m 、第 $n-1$ 个通信周期时的历史信任度 $t_{n-1,i}$ 、本次通信时接收方对其给出的满意度 $S_{n,i}$ 。如果上一次认证为强认证, 则利用预设参数 ω 计算出 $t_{n,i} = e^{-\omega m \tau}$ 。如果上一次认证为简化认证, 首先获得本次通信时接收方设备 j 的信任度系数 δ , 然后利用预设参数 α 计算出 $t_{n,i} = \alpha \cdot \delta \cdot S_{n,i} + (1 - \alpha) \cdot t_{n-1,i}$ 。最终输出第 n 个通信周期时设备 i 的

信任度 $t_{n,i}$ 。

(3) 简化认证申请生成

在LEO卫星对设备进行认证时, 设当前通信周期为 n , 设备用自身的设备编号 devID_i 、当前通信时间戳 T_n 以及计算的哈希值 $h_{i_n} = \text{Hash}(T_n \| h_{i_{n-1}} \| h_{i_0})$ 构造认证申请 Request_i 发送给LEO卫星。

(4) 简化认证申请验证 (H-Verf)

LEO卫星接收到认证申请后, 首先通过 devID_i 对设备个体进行定位, 验证时间戳 T_n 是否超出有效期, 然后通过同步的 $h'_{i_{n-1}}$ 计算得到 h'_{i_n} , 并与 h_{i_n} 对比来对设备进行认证。如果不一致, 则LEO卫星拒绝与该设备进行通信, 输出 $\perp$ 。如果一致, 则根据 devID_i 获得其信任度 $t_{n,i}$, 若 $t_{n,i} \neq 0$ 且 $t_{n,i}$ 不低于其所属设备类型的信任度阈值 $t_{n,X}$, 则LEO卫星认定该设备属于高信任度设备, 直接认证通过, 输出1; 若 $t_{n,i}$ 低于其所属设备类型的信任度阈值 $t_{n,X}$, 则LEO卫星认定该设备属于低信任度设备, 输出0, 需要进一步执行强认证。

(5) 强认证申请生成

LEO卫星先生成随机数 r 作为挑战值, 连同当前时间戳 T'_n 一并发送给设备 i , 要求设备 i 使用其私钥 SK_i 对时间戳 T'_n 和挑战值 r 进行数字签名。设备 i 收到挑战后首先验证时间戳 T'_n 是否超出有效期, 然后用其私钥 SK_i 对时间戳 T'_n 和挑战值 r 进行数字签名, 输入私钥 d 、时间戳 T'_n 和挑战值 r , 随机选取 $k \in \mathbb{Z}_n^*$, 计算 $K = kG = (x_K, y_K)$, $e_s = \text{Hash}(T'_n \| r, P)$, $v = x_K + e_s \pmod{n}$, $s = (1 + d)^{-1} \cdot (k - vd) \pmod{n}$ 。输出的签名 $\sigma_r = (v, s)$ 。

(6) 强认证申请验证

LEO卫星使用设备 i 的公钥 PK_i 对数字签名进行验证, 输入公钥 PK_i 、挑战值 r 和签名 $\sigma_r = (v, s)$, 计算 $e = \text{Hash}(T'_n \| r, P)$ 和 $t = v + s$, 如果 $t = 0$, 输出 $\perp$ 。否则, 通过 t 与 s 计算曲线上的点 $(x_{K'}, y_{K'}) = s * G + t * P$, 再计算 $R = x_{K'} + e$ 。然后验证 R 与 v 是否相等, 如果相等, 表示验证成功, 则认证通过, 输出1; 否则LEO卫星拒绝与该设备进行通信, 输出 $\perp$ 。

需要说明的是, 大型数据传输设备需要与LEO卫星之间建立长时间的稳定通信连接, 报文

数据量大, 因此一颗LEO卫星在其通过该设备的时间窗口期内, 存在无法完成所有数据传输任务的现象, 需要下一颗LEO卫星能够快速接管通信任务完成切换。假设所有LEO卫星组成的星座可以全周期覆盖所有终端设备的工作区域, 并且所有LEO卫星在太空中彼此之间相对位置保持固定。为减少切换认证开销, 采用借助GEO卫星的安全上下文传递机制。在认证过程中, GEO卫星用于检测当前LEO卫星覆盖面积与大型数据传输设备的相对位置。在通信过程中, 如果当前LEO卫星的覆盖面积即将脱离该设备工作区域, GEO卫星作为中继将该设备的安全上下文传递给下一颗将要覆盖该设备工作区域的LEO卫星 (做好切换准备), 使该设备进入下一颗LEO卫星覆盖区域时可快速触发切换, 如图3所示。

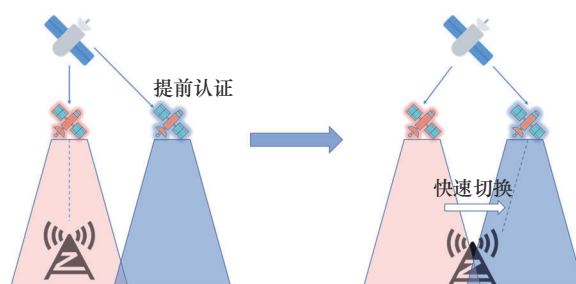


图3 大型数据传输设备提前认证和快速切换示意图

Figure 3 Diagram of authentication in advance and fast handover for large data transmitting devices

与大型数据传输设备类似, 高速移动终端设备同样需要与LEO卫星之间进行较长时间的数据通信, 区别是该类型设备始终在高速移动过程中, 在脱离上一颗LEO卫星覆盖范围后, 之后处在哪颗LEO卫星的覆盖范围内有一定不可预测性。为此, 仍然借助GEO卫星检测当前LEO卫星覆盖面积与高速移动终端设备的相对位置, 由GEO卫星作为中继将该设备的安全上下文提供给当前LEO卫星周围的8颗LEO卫星 (做好切换准备)。当该设备进入任意一颗相邻的LEO卫星覆盖区域时可快速触发切换, 如图4所示。

5 分析与实验

5.1 非形式化安全性分析

针对前述安全目标, 本文对TRE-DA协议的信任评估和认证过程非形式化安全性分析如下。

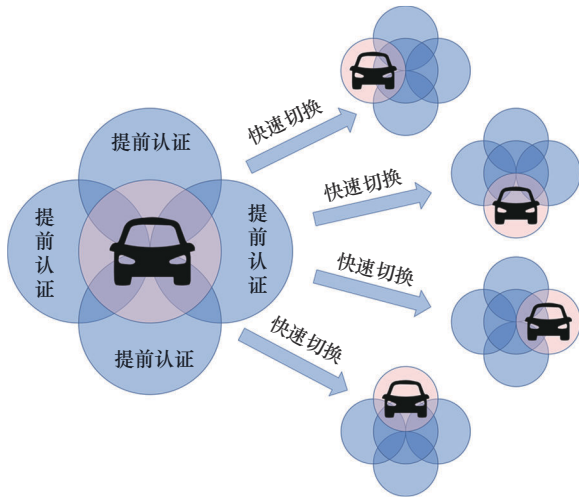


图4 高速移动终端设备提前认证和快速切换示意图

Figure 4 Diagram of authentication in advance and fast handover for high-speed moving terminal devices

(1) 信任评估的可信性

在信任评估过程中，通过对不同设备类型的数据通信特性进行分析，按照直接信任和间接信任建立与各种设备类型相适配的信任评估机制，信任评估机制的实施能够限制不同恶意节点过度占用通信资源的行为，防止分布式拒绝服务（distributed denial of service, DDoS）等攻击的发生。

(2) 不可伪造性

TRE-DA 协议采用哈希链技术结合 SM2 算法，防止发送数据的设备身份被篡改，从而确保不可伪造性。针对简化认证，TRE-DA 协议利用哈希链技术的抗碰撞性，保证敌手无法伪造一个请求通过认证。针对强认证，TRE-DA 协议利用 SM2 算法签名的 EUF-CMA 安全性，确保敌手无法伪造签名通过认证。

(3) 数据完整性

敌手可能篡改消息和实施恶意攻击，导致通信数据被破坏。TRE-DA 协议利用哈希链技术的抗碰撞性，以及 SM2 算法签名的不可伪造性，保证设备发送的数据与 LEO 卫星接收的数据是一致的，若出现不一致则无法通过验证，从而保证数据完整性。

(4) 抗重放攻击

在认证过程中，通过引入时间戳机制保证认证请求的新鲜性，确保认证消息只在特定时间窗

口内有效，从而防止敌手发送 LEO 卫星已经接收过的消息来达到欺骗 LEO 卫星通过认证的目的。

(5) 不可抵赖性

LEO 卫星对不同设备类型终端进行认证时，如果设备因遭受攻击等原因产生了不良通信行为，如发送伪造或错误的无效数据包，会导致自身信任度下降，迫使其采用基于数字签名的挑战—应答这一更强的认证手段，从而防止低信任度设备的抵赖行为。

5.2 形式化安全性分析

本文同时采用了形式化分析工具 Tamarin，选取 Dolve-Yao 安全模型来刻画敌手的能力，对 TRE-DA 协议进行仿真分析和辅助验证。协议的验证通过 Tamarin 工具脚本自动化分析完成，输出路径设置为启发式最优路径。在实际的系统描述中，信任度的判定无法直接进行形式化刻画，本文将协议分为简化认证和强认证两部分分别进行安全性分析，强化认证时 Tamarin 的运行输出如图 5 和图 6 所示。首先验证了协议的可执行性，即协议的所有步骤都能够按照协议要求正确执行。其次验证了协议的单向认证性，协议满足存活性、弱一致性、非单射一致性和单射一致性，与之前非形式化安全性分析得出的协议满足不可伪造性、数据完整性、抗重放攻击的结果一致。

```
summary of summaries:
analyzed: Hash.spthy
executability (exists-trace): verified (6 steps)
aliveness (all-traces): verified (4 steps)
weakagreement (all-traces): verified (4 steps)
noninjectiveagreement (all-traces): verified (4 steps)
injectiveagreement (all-traces): verified (8 steps)
```

图5 简化认证时 Tamarin 的运行输出

Figure 5 Running output of Tamarin with simplified authentication

```
summary of summaries:
analyzed: Sign.spthy
executability (exists-trace): verified (8 steps)
aliveness (all-traces): verified (6 steps)
weakagreement (all-traces): verified (10 steps)
noninjectiveagreement (all-traces): verified (16 steps)
injectiveagreement (all-traces): verified (44 steps)
```

图6 强认证时 Tamarin 的运行输出

Figure 6 Running output of Tamarin with strong authentication

5.3 仿真实验

本文在 Intel i7-10700@2.90 GHz CPU, 32 GB RAM 的实验环境中，分别对信任评估机制和接入认证协议进行仿真实验。

在信任评估机制仿真实验中,总通信周期数设为100,将其中10~20和60~70部分周期置为低通信满意度阶段,其他部分周期置为高通信满意度阶段。本文首先针对信任度评估机制中的各个预设参数 α 和 β 、 γ 进行取值优化,经过选取多组参数开展模拟实验,得到在 α 和 $\beta + \gamma$ 的取值为0.15左右时,3种设备类型的信任度变化最为合理,呈现“快降慢升”的变化趋势。在上述取值条件下,将使用本文提出的信任评估机制与未使用信任评估机制直接将通信满意度作为信任度进行对比,得到海量静态传感器设备类型和大型数据传输设备类型(高速移动终端设备类型与之类似)信任度变化对比分别如图7和图8所示。

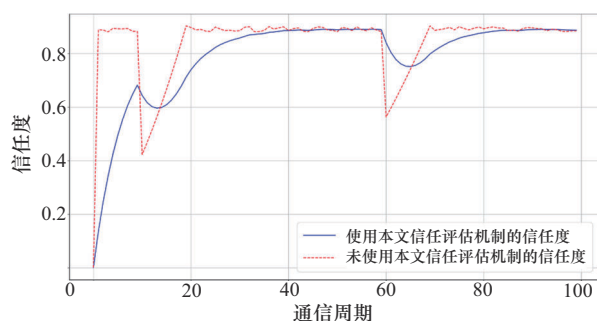


图7 海量静态传感设备类型信任度变化对比

Figure 7 Comparison of trust degree changes for massive static sensing device type

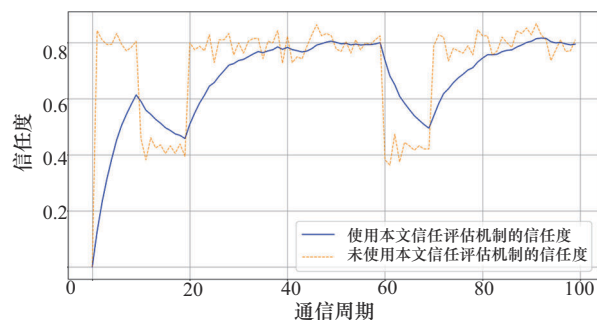


图8 大型数据传输设备类型信任度变化对比

Figure 8 Comparison of trust degree changes for large data transmitting device type

可见,在10~20和60~70周期期间,由于处于低通信满意度阶段,所有设备的信任度都明显出现了下降的情况,在其他阶段随着通信满意度回升,信任度重新回归较高水平。但未使用信任评估机制,直接将通信满意度作为信任度,其曲线振荡较明显,存在急剧下降的现象,这将导

致在后续认证过程中因信任度不足而频繁触发采用开销更大的基于数字签名的强认证机制。而本文提出的信任评估机制由于考虑了历史信任度,其曲线变化较为平滑,不会因短时间内的通信满意度不佳而剧烈变化,在后续认证过程中仍可以采用开销较小的基于哈希链的简化认证机制。

在接入认证协议仿真实验中,本文对3种设备类型的接入认证过程进行模拟,以分析节点数量对认证时延的影响,并对比使用强认证及简化认证机制(即采用本文提出的TRE-DA协议)和仅使用强认证机制(即直接采用基于数字签名的挑战-应答认证机制)的认证时延。仍将总通信周期数设为100,选取10组节点数量(从100~1 000,取值间隔为100),其中,海量静态传感设备类型占50%,大型数据传输设备类型和高速移动终端设备类型各占25%,将直接信任中信任度衰减的预设参数 ω 取值为0.03,间接信任中的预设参数 α 和 $\beta + \gamma$ 仍取值为0.15,各种设备类型的信任度变化和取值范围也如图7和图8所示。

在使用强认证及简化认证机制和仅使用强认证机制两种情况下,设备节点数量变化时的总体认证时延对比如图9所示。可见,随着节点数量的增加,认证时延都在增长,但使用强认证及简化认证机制的设备,在其信任度高于信任度阈值时可采用哈希链技术快速通过认证,由于公钥运算开销远大于哈希运算,总体认证时延明显低于仅使用强认证机制,并且随着节点规模的增大,差距也在随之扩大。实验表明本文提出的基于信任评估的认证方法及协议能够降低总体认证开销,利用信任简化认证流程。

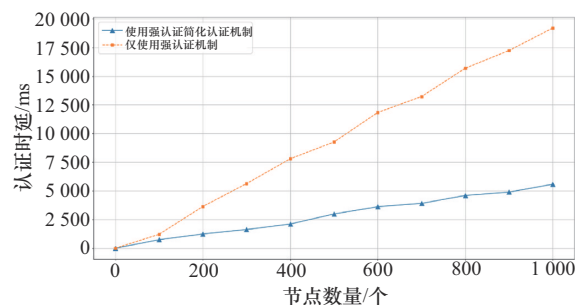


图9 设备节点数量变化时的总体认证时延对比

Figure 9 Comparison of overall authentication delays when the number of device nodes changes

6 结束语

针对增强现有认证机制灵活性和卫星物联网差异化的安全认证需求, 本文提出了卫星物联网终端信任评估机制。针对曾经强认证的终端短时间内再次认证, 和经由强认证节点授信两种情形, 按照直接信任和间接信任刻画了动态调整的信任度量和评估模型。在此基础上, 采用哈希链和 SM2 数字签名技术, 设计了基于信任评估的接入认证协议, 根据设备信任度采用相匹配的认证机制, 实现了在同一认证策略框架下为不同终端设备提供差异化的认证服务。使用非形式化方法和 Tamarin 形式化工具对协议安全性进行了全面分析, 通过实验验证了协议能够降低总体认证开销, 且可利用信任简化认证流程。

参考文献:

- [1] AL HOMSSI B, AL-HOURANI A, WANG K, et al. Next generation mega satellite networks for access equality: opportunities, challenges, and performance[J]. IEEE Communications Magazine, 2022, 60(4): 18-24.
- [2] VOULGARIDIS K, LAGKAS T, ANGELOPOULOS C M, et al. IoT and digital circular economy: principles, applications, and challenges[J]. Computer Networks, 2022, 219: 109456.
- [3] CAPEZ G M, HENN S, FRAIRE J A, et al. Sparse satellite constellation design for global and regional direct-to-satellite IoT services[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(5): 3786-3801.
- [4] CHAUDHRY S A, IRSHAD A, KHAN M A, et al. A lightweight authentication scheme for 6G-IoT enabled maritime transport system [J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2401-2410.
- [5] ALHANDI S A, KAMALUDIN H, ALDUAIS N A M. Trust evaluation model in IoT environment: a comprehensive survey[J]. IEEE Access, 2023, 11: 11165-11182.
- [6] XUE K P, MENG W, LI S H, et al. A secure and efficient access and handover authentication protocol for Internet of things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.
- [7] MA R H, CAO J, FENG D G, et al. LAA: lattice-based access authentication scheme for IoT in space information networks[C]//Proceedings of the IEEE Internet of Things Journal. Piscataway: IEEE Press, 2020: 2791-2805.
- [8] MENG W, XUE K, XU J, et al. Low-latency authentication against satellite compromising for space information network[C]//Proceedings of 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2018: 237-244.
- [9] XUE K P, MENG W, LI S H, et al. A secure and efficient access and handover authentication protocol for Internet of things in space information networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 5485-5499.
- [10] YANG Q Y, XUE K P, XU J, et al. AnFRA: anonymous and fast roaming authentication for space information network[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 486-497.
- [11] 曹进, 石小平, 马如慧, 等. 融合双层卫星网络的星地和星间 AKA 协议[J]. 网络与信息安全学报, 2023, 9(1): 18-31.
- CAO J, SHI X P, MA R H, et al. Fusion of satellite-ground and inter-satellite AKA protocols for double-layer satellite networks[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 18-31.
- [12] HUYNH T D, JENNINGS N R, SHADBOLT N R. An integrated trust and reputation model for open multi-agent systems[J]. Autonomous Agents and Multi-Agent Systems, 2006, 13(2): 119-154.
- [13] 王伟, 杨本朝, 吴涛. 贝叶斯预测下的域间路由信任机制[J]. 安徽大学学报(自然科学版), 2014, 38(4): 33-36.
- WANG W, YANG B C, WU T. A trusted inter-domain routing protocol based on Bayesian estimation theory[J]. Journal of Anhui University (Natural Science Edition), 2014, 38(4): 33-36.
- [14] D'ANGELO G, RAMPONE S, PALMIERI F. Developing a trust model for pervasive computing based on apriori association rules learning and Bayesian classification[J]. Soft Computing, 2017, 21: 6297-6315.

[作者简介]



田敏求 (1985-), 男, 河北保定人, 中国科学院信息工程研究所博士生, 主要研究方向为卫星物联网的安全认证与密码应用。



李凤华 (1966-), 男, 湖北浠水人, 博士, 中国科学院信息工程研究所研究员、博士生导师, 主要研究方向为网络与系统安全、隐私计算、信息保护。



李子孚 (1992-), 女, 内蒙古赤峰人, 博士, 中国科学院信息工程研究所高级工程师、硕士生导师, 主要研究方向为网络与系统安全。



郭超 (1987-), 女, 江西九江人, 博士, 北京电子科技学院讲师、硕士生导师, 主要研究方向为卫星通信网络安全。