学号：2023264570

西 北 工 业 大 学

全日制专业学位研究生学位论文
选题报告

学　　院　网络空间安全学院

专业 领域　网络与信息安全

姓　　名　何明轩

学位 级别　硕士

校内 导师　张尚伟

校外 导师　王洪波

报告 日期　2024.11.25

研 究 生 院

全日制专业学位研究生学位论文选题报告的要求

一、 选题要求

1．论文选题应直接来源于生产实际或者具有明确的应用背景和实用价值，可以是一个完整的工程设计项目或技术改造项目，可以是技术攻关研究课题，也可以是新工艺、新设备、新材料、新产品的研制与开发。

2．论文选题应有一定的技术难度、先进性和工作量，能体现作者综合运用科学理论、方法和技术手段解决工程实际问题的能力。

3．论文形式可以是工程设计、研究论文、技术改造或工程管理。无论是那一种论文形式，论文都应至少有局部深入的理论分析。

4. 按照《西北工业大学涉密研究生涉密学位论文的管理规定》要求，硕士（含各类专业学位）学位论文不接受涉密论文的申请，请自行脱密处理。

5．选题报告会应以学术活动的方式公开进行。

二、 正式开题之前，研究生应在广泛阅读中、外文资料的基础上，深入了解拟选课题的国内外研究动态，把握所选课题的目的、意义和预期结果，明确课题工作的设想、方法和研究路径。

三、 研究生在规定的时间内，写出选题报告初稿，经指导教师审阅同意后，由指导教师安排选题报告时间。选题报告未通过者，重新开题，若第二次选题报告仍通不过者，则按有关规定终止学籍。

四、 选题报告不能按期完成者，应及时向研究生院培养处提出延期申请。

五、 本表可以打印或用钢笔认真填写，若不够填写时，可另加附页。

六、 本表可以在计算机上填写、打印，手工填写时须字迹清楚且不得涂改。

七、 表中所列项目必须全部填写，不留空白。

<table>
<tr><td rowspan="5">研究生实习简况</td><td>姓　名</td><td>何明轩</td><td>学　　号</td><td>2023264570</td><td>电　话</td><td>13541361574</td></tr>
<tr><td>实践单位名称</td><td colspan="5">天津天睿科技有限公司</td></tr>
<tr><td>校内导师</td><td colspan="2">张尚伟</td><td>联系方式</td><td colspan="2">18091287899</td></tr>
<tr><td>校外导师</td><td colspan="2">王洪波</td><td>联系方式</td><td colspan="2">16602616364</td></tr>
<tr><td>计划实习时间</td><td colspan="5">2024 年 12 月-2025 年 10 月</td></tr>
<tr><td colspan="2">论文题目</td><td colspan="5">空天地协作多跳网络用户隐匿安全接入方法研究</td></tr>
<tr><td colspan="2" rowspan="2">论文类型
(请在有关项目下作√记号)</td><td>产品研发</td><td>工程设计</td><td>应用研究</td><td>工程/项目管理</td><td>调研报告</td><td>案例分析</td><td>企业诊断</td><td>专题研究</td><td>实践报告</td></tr>
<tr><td></td><td></td><td>√</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

选题依据（选题的国内外背景、目的及意义、应用价值和预期结果）

1.1 国内外背景

随着信息通信技术的快速发展和万物互联时代的到来，传统的地面网络已难以满足日益增长的全球覆盖、高速传输和大规模连接需求。空天地一体化网络（Space-Air-Ground Integrated Network, SAGIN）作为下一代通信网络的重要架构，将空间（卫星）、空中（无人机、高空平台）和地面（基站、用户终端）网络有机结合，形成一个覆盖全球、无缝互联、动态协作的综合通信系统。这种网络不仅能够提供广覆盖、高可靠的通信服务，还能满足多种应用场景（如物联网、智能交通、国防通信等）的需求。如何在万物互联时代保证系统对用户接入的可靠性和安全性，成为当前领域的研究重点。

Wang X 等人[2]利用先进的非正交多址接入（NOMA）、毫米波、可见光通信等技术提高频谱效率和系统容量。其中新兴 NOMA 技术的融入用于满足即将到来的万物互联时代对巨大流量和海量接入的需求[1]。通过将协作通信与 NOMA 技术结合，Ding Z 等人[3]提出了协作 NOMA（C-NOMA），通过将近端用户用作每个 NOMA 组中的中继来增强 NOMA 通信。与传统 NOMA 相比，这种工作方式可以在网络容量上获得更高的性能增益。因此，C-NOMA 技术有望融入 SAGIN，以满足各种潜在 IoE 应用的大规模连接和更高的频谱效率需求[4]。

虽然 SAGIN 网络架构具有众多优势，但在多跳通信和用户协作的复杂环境中，网络面临的安全威胁显著增加，例如用户隐私泄露、数据篡改、中间人攻击等问题。此外，传统的接入认证机制难以兼顾隐匿通信需求和多跳网络的动态特性。尽管 NOMA 技术在未来 SAGIN 中展现出巨大潜力，但不可避免地会带来安全问题，例如隐私信息泄露、伪造攻击等。在典型的 NOMA 组中，接收方可以解码其他用户的最强信号，而且 NOMA 组通常是基于信道质量而非安全性考虑来划分的。因此，每个 C-NOMA 组中的机密或敏感数据可能通过不安全的中继进行传输。为

了解决上述问题，一个可行的研究方向是探索安全接入认证方案。对于空地一体化网络，Chen M 等人[5]针对无线安全协商保护过程研究了一种认证方案。针对 NOMA 通信系统，近期研究工作通常关注物理层认证方案。例如，Zhang Y[6]等人提出了一种利用 NOMA 技术特点和哈希操作不可逆性的群体认证机制，适用于大规模机器类型通信系统。考虑到用户可能与攻击者串通引发的安全问题，Xie N 等人[7]提出了三种物理层认证方案，分别基于共享认证标签、独立叠加认证标签以及时分复用认证标签。在此基础上，他们进一步开发了一种隐私保护认证方案，以提高系统认证性能[7]。

上述方案尚未关注针对量子攻击的安全接入认证问题，特别是在 SAGIN 中。因此，研究人员倾向于基于后量子密码学机制改进接入认证方案。例如，Wang Y 等人[8]将数字理论研究单元（NTRU）方案引入密钥生成过程，设计了一种基于格的匿名接入认证方案

同时上述接入认证方案也仅仅实现了单次认证的功能，为了实现永不信任，持续认证的功能，Liu X 等人[9]设计了一种基于零知识证明的非交互式轻量级认证协议，用于保护卫星通信场景下物联网设备的安全。Yantao Z 等人[10]提出了一种基于零知识证明和智能合约的分散匿名认证方案，用以防止恶意用户的攻击。

现有的无线认证接入方案主要为正交多址接入（OMA）通信系统设计，针对 SAGIN 场景下的认证方案较少考虑隐匿通信以及持续认证，针对 NOMA 通信的方案较少考虑量子攻击，因此本设计结合后量子算法 NTRU、Tor 网络以及零知识认证，在 SAGIN 场景下具有抗量子攻击、隐匿通信以及持续验证的特性，具有一定的创新性以及现实意义。

1.2 选题目的及意义

项目的目的:本项目旨在针对空天地协作多跳网络，设计一种支持用户隐匿的安全接入方法，确保用户接入的私密性和数据传输的安全性。并结合零知识证明，提出持续认证接入方案，对用户的身份进行持续验证，以确保用户的合法性。

项目的意义：本设计提出的隐匿接入方法能够有效抵御多种安全威胁（如隐私泄露和伪造攻击），提升空天地网络在敏感场景中的适用性，如军事通信和关键基础设施监控；方法将会有高效的认证机制，不仅能够减少通信延迟，还能适应空天地协作多跳网络的动态特性，满足未来大规模接入场景需求；本研究的成果后续可以进行修改实装至真实的卫星系统的实际场景上，为包括地球观测卫星、导航卫星和通信卫星在内的多种场景提供安全接入支持。

1.3 预期结果

（1)拟设计一种基于 NTRU 的自适应单次安全认证方案,用于 SAGIN 中的 C-NOMA 通信，综合考虑可信和不可信中继，用于卫星与用户之间的单次认证以及单次安全通信。

（2）拟设计一种基于洋葱网络（Tor）的用户隐匿通信网络，结合 ShorTor 协议（一种用于 Tor 网络的增量协议）在保证匿名性的同时，用以显著降低 Tor 网络的延迟以达到用户正常使用的延迟水平。

（3）拟将上述隐匿通信网络以及单次安全认证方案同零知识证明相关技术进行结合，完成基于零知识证明的持续认证接入方案。

二、研究内容、研究方案、工作量的估计，存在问题及拟采取的解决措施

2.1 研究内容

（1）基于 NTRU 算法的空天地一体化网络接入单次安全认证方案

单次安全认证方案的网络模型是空天地协作多跳网络 SAGIN，针对 SAGIN 内中的信任和不信任 NOMA 中继拟设计一个安全接入认证协议，协议采用了数字证书技术用以交换用户与卫星之间的公钥并相互验证双方身份，采用 NTRU 后量子算法以抵抗针对 C-NOMA 通信的量子攻击，在保障通信双方信息安全性的前提下，提高网络的接入效率和用户体验。同时方案还需要经过形式化验证分析，证明其正确性以及安全性。最后方案需要进行性能测试，并与各类目前已有的单次认证方案进行性能对比分析。

（2）基于 Tor 的空天地一体化网络匿名接入认证方案

隐匿通信网络以 Tor 洋葱网络为基石，通过在用户和目标服务器之间建立一个多跳路径，采用分层加密（类似洋葱的结构）对数据进行保护。每一跳的中继节点只能解密属于自己的一层加密，从而无法获知通信双方的完整信息。同时本方案拟应用 ShorTor 协议，由 Tor 中继运行，使其独立于 Tor 客户端执行的路径选择，从而大幅降低网络延迟，同时保留了 Tor 现有的安全属性。最后方案需要进行性能测试，并与目前已有的 Tor 方案进行性能对比分析。

（3）基于零知识证明的空天地一体化网络持续认证接入方案

持续认证接入方案采用零知识证明（ZKP）机制，用户在不泄露其身份或敏感信息的情况下，向认证系统证明其合法性。通过零知识证明技术，用户能够动态地证明自己拥有合法接入权限，而无需暴露关键身份信息或重新提交完整认证数据。其优势是存在动态安全性，持续认证机制能够有效应对动态环境中身份伪造、凭证失效等问题，确保接入过程的持续安全。同时零知识证明隐藏了用户身份信息，使得认证服务器和中继节点无法获取用户敏感数据。方案的具体流程分为初次认证以及持续认证，初次认证即使用前面部分提到的匿名单次接入认证方法，持续认证是在用户接入之后，定期触发基于零知识证明的动态认证请求。随后对方案进行安全性分析，主要是对零知识证明部分进行安全验证。最后进行仿真模拟实验，测试方案整体的性能，并与其余同类型方案进行对比。

2.2 研究方案

(1) 单次匿名安全接入认证方案

首先针对空天地协作多跳网络架构进行分析。研究内容包括 SAGIN 的协作特性和多跳通信模式，包括卫星、无人机和地面节点的角色分工与通信流程，并给出具体的网络通信系统模型。如图 1 所示，我们考虑一个典型的 SAGIN 下行链路功率域 NOMA 网络系统，其中包含卫星、无人机（UAV）和地面用户。

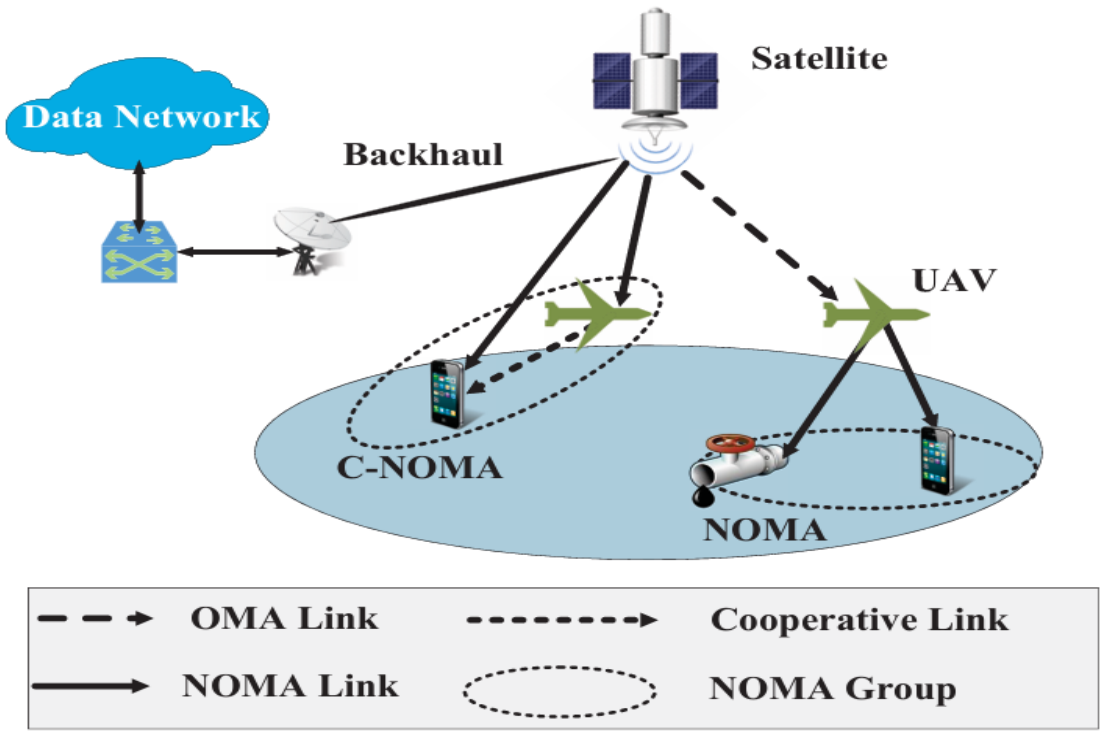

图 1. 空天地一体化 NOMA 系统示意图

随后我们需要设计安全接入方法的具体流程，该流程分为两个部分。

1)系统建立部分：该部分将会初始化各个节点（例如卫星、用户）的初始参数，完成系统的初步建立。

2)节点交互部分：构建各节点之间的交互过程，该过程使用流程图来进行，交互结束即代表节点之间完成了匿名安全接入过程。安全 NOMA 通信机制图如图 2 所示。目前已设计的不信任模式的交互图如图 3 所示。

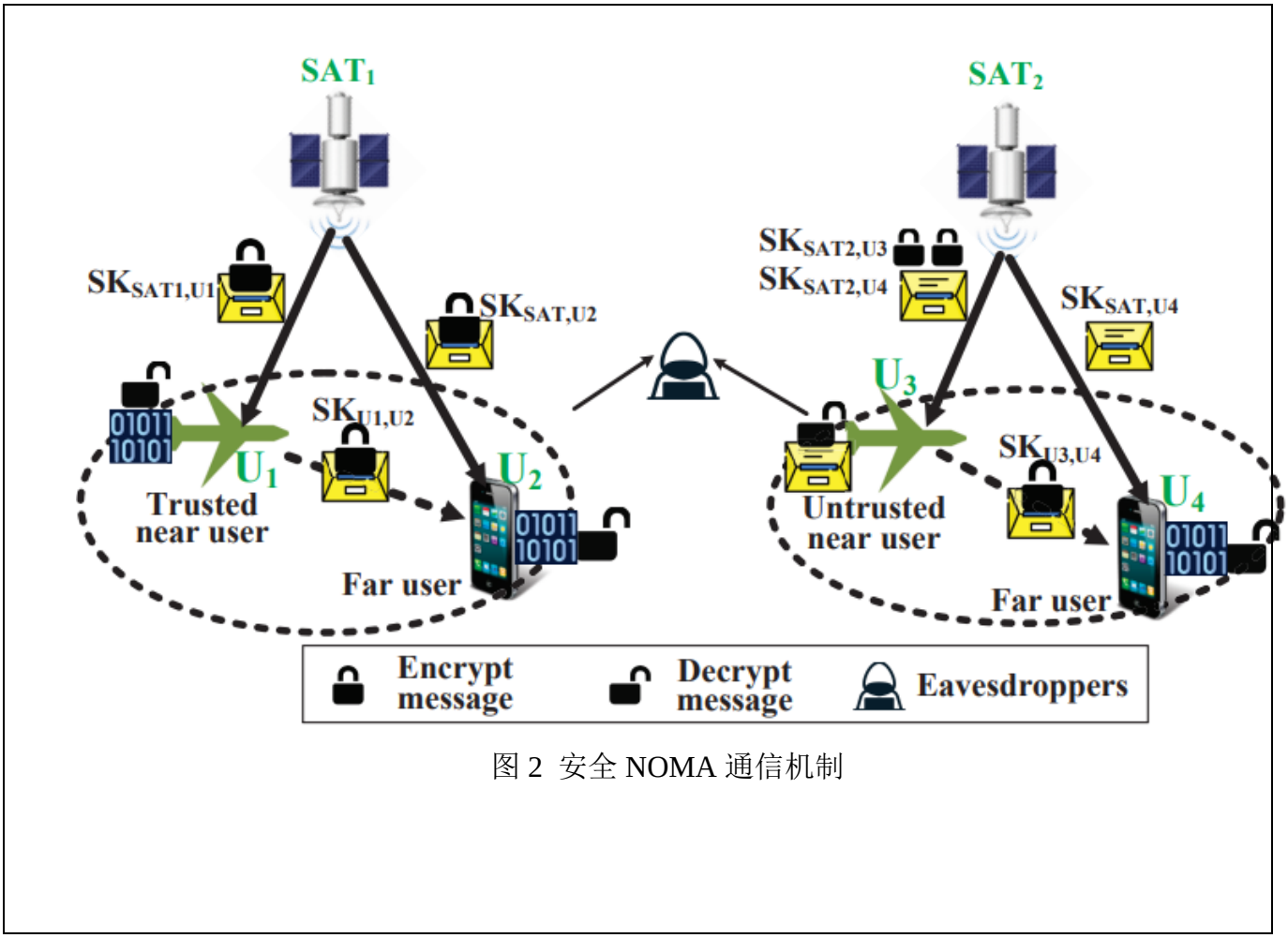

图 2 安全 NOMA 通信机制

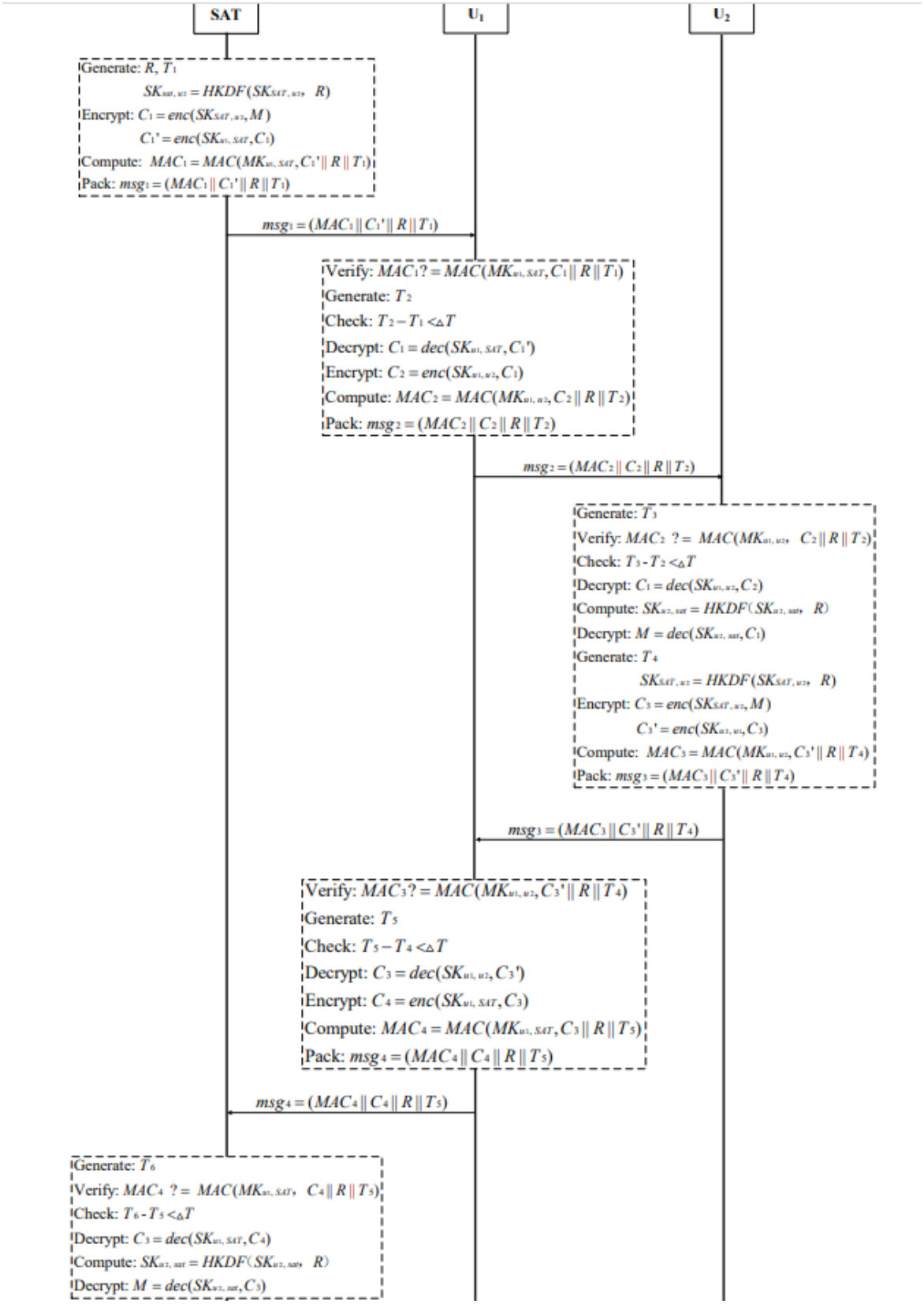

图 3 不信任模式交互图

隐匿通信保护：在数据传输阶段，认证凭证及相关通信数据通过 Tor 网络进行传输，确保通信行为不可被检测，通信双方不会暴露自己的身份信息。Tor 网络中通过多跳中继掩盖用户的真

实位置，确保认证过程和后续通信的数据内容不会被第三方截获或分析。同时还会使得认证行为难以被检测，即使流量被拦截，也无法区分正常流量和认证流量。

然后我们将对该上述提到的安全接入方法进行形式化验证分析，拟采用 Proverif 或者 Avispa 形式化验证工具进行分析，对设计出的安全协议在 Dolev-Yao 威胁模型下进行双向身份认证。在 Dolev-Yao 威胁模型中，攻击者几乎无所不能，可以想象成，我们每个人在网络中通信都是在和攻击者通信，收到网络里发来的消息也都是攻击者发送给我们的消息。我们的通信安全主要依赖于密码学的安全保护。因此采用 Dolev-Yao 威胁模型可以充分有效地模拟攻击者的绝大多数攻击行为，对该加密协议进行充分的测试。

随后我们需要对整个认证流程进行逻辑化验证，拟采用 Ban 逻辑来进行验证。BAN 逻辑是一种基于知识和信任的形式逻辑分析方法，由 Burrows，Abadi 和 Needham 提出，通过对认证协议的运行进行形式分析，从协议执行者最初的一些基本信仰出发，根据协议执行的每个参与者发出和收到的消息，推理得到参与者的最终信仰。应用 BAN 逻辑对认证协议进行分析，首先需要进行理想化处理，将协议的消息转换成 BAN 逻辑中的公式，再根据具体情况进行合理假设，由逻辑的推理法则根据理想化协议和假设进行推理，推断协议能否完成预期的目标。如果在协议流程结束时能够建立关于共享通信密钥、对方身份等的信任，则表明协议是安全的。

(2)基于零知识证明的持续认证接入方法

初次认证：用户通过上述提出的单次认证方法，与认证服务器（如认证机构 CA）建立初始信任。认证过程中采用消息认证码技术生成一次性凭证，结合零知识证明的身份验证机制，完成用户合法性初始认证。在 NOMA 接入场景中，用户身份信息被隐藏，认证凭证与信道资源动态绑定。

持续认证：用户接入后，认证服务器不定期触发基于零知识证明的动态认证请求。用户通过 ZKP 技术向服务器证明其对初始认证凭证的合法持有，而无需暴露凭证本身。随着信道质量的变化，持续认证可以动态调整信道分配和功率分配策略，确保 NOMA 多用户通信的效率和安全性。

最后我们还要对所提出的安全持续认证接入方法进行仿真模拟实验，初步计划是使用两台基于 Intel Core i5-13400F CPU，使用 Ubuntu 操作系统的计算机来进行仿真实验。仿真实验完成后拟将实验环境改为真实的卫星以及无人机平台来进行实际的通信实验，以测量各种性能参数。我们需要测量平均计算开销、配置密钥参数的时间、协议交互的总的数据交换量、密码运算的时间开销等参数。并与其他匿名验证方法进行性能对比以及进行结果分析。

2.3 存在问题及解决措施

(1)基于 Tor 的单次匿名安全接入认证方案设计

解决措施：重新阅读关于 Tor 网络和 ShorTor 协议的底层代码，理清项目内的各个板块的逻辑，在单次认证部分的代码之上完成隐匿通信功能，使之形成一个完整的项目。

(2)基于零知识证明的可持续接入认证方案设计

解决措施：首先学习零知识证明的基本概念、分类、性质（如完备性、可靠性和零知识性），从理论入门。再深入学习 ZKP 的算法和框架，研究常见的零知识证明算法， Schnorr 协议（适合身份认证）以及 zk-STARK（抗量子攻击的零知识证明）。最后在 Circom 零知识证明编译器中进行技术实践。

三、论文进度安排

阶段 1：文献调研与需求分析（1 个月）

系统调研隐匿通信技术、接入认证机制及相关理论背景；调查空天地协作多跳网络的体系架构、技术特点及安全需求；学习后量子密码学技术（NTRU 算法）在隐匿通信中的应用。

阶段 2：隐匿安全接入模型设计（3 个月）

构建适用于空天地协作多跳网络的隐匿安全接入系统模型，基于信任等级动态选择中继节点，设计自适应多跳协作认证机制；将零知识证明（ZKP）技术嵌入认证机制，以实现持续认证功能。

阶段 3：算法实现与优化（3 个月）

实现基于 NTRU 的后量子安全认证算法，构建抗量子攻击的密钥管理机制；设计并实现身份隐匿协议，将零知识证明应用于用户身份认证过程；对算法进行优化，减少计算复杂度，提高认证效率。

阶段 4：仿真与性能评估（3 个月）

搭建仿真实验环境，模拟空天地协作多跳网络中的通信场景；验证所设计隐匿安全接入方法的有效性、隐匿性、安全性及抗量子攻击能力；分析认证效率、延迟、能耗及网络性能，优化算法参数；同时完成形式化验证分析部分。

阶段 5：总结与论文撰写（2 个月）

整理研究内容，撰写硕士论文；准备答辩材料，修改完善论文内容。

共计：12 个月

四. 参考文献

[1] C. -X. Wang *et al.*, "On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905-974, Secondquarter 2023, doi: 10.1109/COMST.2023.3249835.

[2] X. Wang, H. Chen and F. Tan, "Hybrid OMA/NOMA Mode Selection and Resource Allocation in Space-Air-Ground Integrated Networks," in IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2024.3452477.

[3] Z. Ding, M. Peng and H. V. Poor, "Cooperative Non-Orthogonal Multiple Access in 5G Systems," in IEEE Communications Letters, vol. 19, no. 8, pp. 1462-1465, Aug. 2015, doi:

10.1109/LCOMM.2015.2441064.

[4] P. Qin, M. Fu, Y. Fu, R. Ding and X. Zhao, "Collaborative Edge Computing and Program Caching With Routing Plan in C-NOMA-Enabled Space-Air-Ground Network," in IEEE Transactions on Wireless Communications, doi: 10.1109/TWC.2024.3464610.

[5] M. Chen, S. Guo, X. Huang, L. Su and H. Du, "Research on Secure Access in Converged Satellite and Terrestrial Networks," 2023 IEEE 31st International Conference on Network Protocols (ICNP), Reykjavik, Iceland, 2023, pp. 1-6, doi: 10.1109/ICNP59255.2023.10355610.

[6] Y. Zhang, H. Wu, Z. Wei, Q. Gao, N. Zhang and X. Tao, "Physical Layer Group Authentication in mMTC Networks with NOMA," 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 2021, pp. 1-6, doi: 10.1109/WCNC49053.2021.9417518.

[7] N. Xie, S. Zhang and A. X. Liu, "Physical-Layer Authentication in Non-Orthogonal Multiple Access Systems," in IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1144-1157, June 2020, doi: 10.1109/TNET.2020.2979058.

[8] Y. Wang, W. Zhang, X. Wang, M. K. Khan and P. Fan, "Security Enhanced Authentication Protocol for Space-Ground Integrated Railway Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 1, pp. 370-385, Jan. 2024, doi: 10.1109/TITS.2023.3307453. R. Wang, S. Zhang, B. Yang, Z. Yang, P. Zhang and D. Wu, "Enabling Data Sharing Through Data Trusts in LEO Satellite Internet," in IEEE Wireless Communications, vol. 31, no. 1, pp. 70-76, February 2024, doi: 10.1109/MWC.013.2200233.

[9] X. Liu, A. Yang, C. Huang, Y. Li, T. Li and M. Li, "Decentralized Anonymous Authentication With Fair Billing for Space-Ground Integrated Networks," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7764-7777, Aug. 2021, doi: 10.1109/TVT.2021.3091775.

[10] Z. Yantao and M. Jianfeng, "A highly secure identity-based authenticated key-exchange protocol for satellite communication," in Journal of Communications and Networks, vol. 12, no. 6, pp. 592-599, Dec. 2010, doi: 10.1109/JCN.2010.6388306.

[11] Zhou Y , Wang L .A Lattice-Based Authentication Scheme for Roaming Service in Ubiquitous Networks with Anonymity[J].Security and Communication Networks, 2020, 2020(3):1-19.DOI:10.1155/2020/2637916.

[12] Burrows M , Abadi M , Needham R M .A logic of authentication[J].Acm Transactions on Computer Systems, 1989, 23(5):1-13.DOI:10.1145/74851.74852.

[13] X. Li et al., "Physical-Layer Authentication for Ambient Backscatter-Aided NOMA Symbiotic Systems," in IEEE Transactions on Communications, vol. 71, no. 4, pp. 2288-2303, April 2023, doi: 10.1109/TCOMM.2023.3245659.