软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software [doi: 10.13328/j.cnki.jos.006514]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于雾计算的智能医疗三方认证与密钥协商协议*

王菲菲[1], 汪 定[2,3]

[1](重庆邮电大学 网络空间安全与信息法学院, 重庆 400065)

[2](南开大学 网络空间安全学院, 天津 300350)

[3](天津市网络与数据安全技术重点实验室 (南开大学), 天津 300350)

通信作者: 汪定, E-mail: wangding@nankai.edu.cn

摘 要: 在智能医疗中, 将云计算技术与物联网技术结合, 可有效解决大规模医疗数据的实时访问问题. 然而, 数据上传到远程云服务器, 将带来额外的通信开销与传输时延. 借助雾计算技术, 以终端设备作为雾节点, 辅助云服务器在本地完成数据存储与访问, 能够实现数据访问的低延迟与高移动性. 如何保障基于雾计算的智能医疗环境的安全性成为近期研究热点. 面向基于雾计算的智能医疗场景, 设计认证协议的挑战在于: 一方面, 医疗数据是高度敏感的隐私数据, 与病人身体健康密切相关, 若用户身份泄漏或者数据遭到非法篡改将导致严重后果; 另一方面, 用户设备和雾节点往往资源受限, 认证协议在保护用户隐私的同时, 需要实现用户、雾节点、云服务器之间的三方数据安全传输. 对智能医疗领域两个具有代表性的认证方案进行安全分析, 指出 Hajian 等人的协议无法抵抗验证表丢失攻击、拒绝服务攻击、仿冒攻击、设备捕获攻击、会话密钥泄漏攻击; 指出 Wu 等人的协议无法抵抗离线口令猜测攻击、仿冒攻击. 提出一个基于雾计算的智能医疗三方认证与密钥协商协议, 采用随机预言机模型下安全归约、BAN 逻辑证明和启发式分析, 证明所提方案能实现双向认证与会话密钥协商, 并且对已知攻击是安全的; 与同类方案的性能对比分析表明, 所提方案显著提高了安全性, 并具有较高的效率.

关键词: 认证协议; 智能医疗; 雾计算; 密钥协商; 物联网

中图法分类号: TP309

中文引用格式: 王菲菲, 汪定. 基于雾计算的智能医疗三方认证与密钥协商协议. 软件学报. http://www.jos.org.cn/1000-9825/6514.htm

英文引用格式: Wang FF, Wang D. Fog Computing-based Three-party Authentication and Key Agreement Protocol for Smart Healthcare. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/6514.htm

Fog Computing-based Three-party Authentication and Key Agreement Protocol for Smart Healthcare

WANG Fei-Fei[1], WANG Ding[2,3]

[1](School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

[2](College of Cyber Science, Nankai University, Tianjin 300350, China)

[3](Tianjin Key Laboratory of Network and Data Security Technology (Nankai University), Tianjin 300350, China)

Abstract: In smart healthcare, cloud computing and the Internet of Things are combined to solve the problem of real-time access to large-scale data. However, the data is uploaded to a remote cloud. It increases additional communication cost and transmission delay. Fog computing has been introduced into smart healthcare to solve this problem. The fog servers assist the cloud server to complete data storage and access locally. It contributes to low latency and high mobility. Since the medical data is highly sensitive, how to design a fog computing-based smart healthcare authentication protocol has become a research hotspot. If the data is tampered illegally, the consequences will be catastrophic. Hence, the authentication protocol should be secure against various attacks and realize the secure data transmission

* 基金项目: 国家自然科学基金 (62172240); 南开大学百名青年学科带头人计划 (9920200010)
收稿时间: 2021-05-20; 修改时间: 2021-08-30; 采用时间: 2021-10-09

among users, fog nodes, and cloud servers. This study analyzes two schemes for smart healthcare, and points out that Hajian *et al.*'s scheme cannot resist stolen verifier attack, denial of service attacks, impersonation attacks, node capture attack, and session key disclosure attacks; Wu *et al.*'s scheme cannot resist offline password guessing attacks and impersonation attacks. Furthermore, a fog computing-based three-party authentication and key agreement protocol are proposed for smart healthcare. The security is proved by using the random oracle model, the BAN logic, and heuristic analysis. As result, it is secure against known attacks. The performance comparison with related schemes shows that the proposed scheme is more suitable for fog computing-based smart healthcare.

Key words: authentication protocol; smart healthcare; fog computing; key agreement; Internet of Things (IoT)

1 引 言

随着移动通信技术与无线传感技术的发展, 物联网技术[1]广泛应用于智能医疗领域, 实现对病人身体健康的实时监测[2]. 然而, 面对日益增长的数据量, 医疗传感设备有限的计算和存储能力成为制约其发展的关键因素[3,4]. 云计算技术[5]作为一种新的服务范式被引入智能医疗领域. 云计算能够高效、便捷地实现信息和资源共享[6−8]. 在云计算环境中, 传感设备收集的数据上传到远程云服务器, 云服务器对数据进行存储与分析, 用户通过访问云服务器获取数据, 在这个过程中势必带来额外的通信开销与传输时延[9]. 借助雾计算技术[10], 利用位于网络边缘的网关、访问点作为雾节点, 辅助云服务器在本地完成数据的存储与分析, 能够有效缓解该问题[11]. 在雾计算环境下, 雾节点部署在无人值守环境, 加之通信环境具有脆弱性, 容易遭受各种攻击. 认证与密钥协商协议对于实现医疗数据的安全访问和安全传输、保护用户隐私是至关重要的.

在雾计算辅助的智能医疗场景中, 病人身上佩戴着各种医疗传感设备, 用于收集病人的血压、脉搏、呼吸频率等生理健康信息. 医疗传感设备将收集到的医疗信息汇聚到远程云服务器, 位于网络边缘的雾节点辅助云服务器完成数据的存储与处理. 基于雾计算的智能医疗认证协议具有以下特点: 首先, 实现用户、雾节点、云服务器之间的三方密钥协商, 相比两方密钥协商更复杂. 其次, 智能医疗场景对会话密钥的安全性有更高的要求. 智能医疗场景中传输的数据具有高度敏感性, 若发生数据篡改, 将发生难以想象的后果, 为保证数据的安全传输, 所建立的会话密钥应能抵抗已知攻击, 包括临时秘密值泄漏攻击、满足前向安全性. 再次, 雾节点部署在无人值守环境, 攻击者可捕获设备并提取密钥, 应保证雾节点被攻破时, 对其他通信方及会话密钥的安全性不产生影响.

1.1 相关工作

2012 年, Wu 等人[12]提出一个适用于远程医疗信息系统的认证方案.然而, 该方案仅以用户口令作为认证因素, 鉴于口令存在被攻破的可能性, 不能有效防止未经授权的访问. 在用户身份认证中使用新的认证因素, 例如生物特征, 智能卡, 能够有效提高身份认证的安全性, 认证方案使用两个或两个以上认证因素成为一种趋势[13]. 2013 年, He 等人[14]提出一个适用于病人监测的无线医疗传感器网络双因素认证方案, 为用户访问可穿戴传感设备收集患者信息提供安全保护. 然而 Li 等人[15]指出 He 等人[14]方案无法抵抗离线口令猜测攻击和仿冒攻击. 2017 年, Li 等人[16]提出一种集中式两跳无线人体局域网匿名认证方案, 该方案实现传感设备身份匿名性等安全特性. 但随后 Koya 等人[17]指出 Li 等人[16]方案易遭受传感设备仿冒攻击. Wu 等人[18]提出一种基于云的可穿戴设备认证协议, 但该方案使用昂贵的双线性对运算, 涉及较高的计算开销. Das 等人[19]提出一种基于生物特征的可穿戴传感设备认证协议, 引入生物特征增强用户身份认证的安全性.

2018 年, Wu 等人[20]提出一种轻量级的无线医疗传感器网络双因素认证方案, 声称该方案能够抵抗已知攻击, 但该方案未能实现前向安全性. Wazid 等人[21]提出一种基于生物特征的无线体域网认证与密钥管理协议, 使用模糊提取器[22]提取用户生物特征. Amin 等人[23]提出一个适用于病人监测的基于哈希函数的无线医疗传感器网络认证方案, 然而该方案存在严重的安全缺陷, 例如重放攻击、仿冒攻击、拒绝服务攻击、会话密钥泄漏攻击. 2019 年, Gupta 等人[24]提出一个轻量级的可穿戴传感设备认证与密钥协商方案, 在传感设备注册阶段无需使用安全信道, 具有良好的可扩展性. 2019 年, 为解决用户访问远程云数据中心的传输时延问题, Jia 等人[25]提出一个基于双线性对的无线医疗传感器网络认证方案, 借助雾计算技术实现数据的本地访问与存储. 2020 年, 为实现前向安全性与用户身份标识不可追踪性, Fotouhi 等人[26]提出一个基于哈希链技术的无线人体局域网认证协议. Hajian

等人[27]指出 Gupta 等人[24]方案未实现前向安全性, 不能抵抗离线口令猜测攻击与仿冒攻击, 并提出一个新的改进方案. 2021 年, Wu 等人[28]指出 Jia 等人[25]方案未能实现本地口令验证, 不能抵抗临时秘密值泄露攻击, 提出一个新的改进方案.

1.2 本文贡献

智能医疗是典型的安全攸关应用场景, 要求认证协议具有高安全性. 本文对两个典型的智能医疗认证协议的安全分析表明, 现有方案难以为智能医疗场景提供所需的安全保护. 提出一个基于雾计算的智能医疗三方认证与密钥协商协议, 为智能医疗数据的访问和传输, 提供安全保护. 本文的贡献如下.

(1) 对 Hajian 等人[27]协议和 Wu 等人[28]协议进行安全分析. 指出 Hajian 等人[27]协议无法抵抗验证表丢失攻击、拒绝服务攻击、仿冒攻击、设备捕获攻击、会话密钥泄漏攻击; 指出 Wu 等人[28]协议无法抵抗离线口令猜测攻击、仿冒攻击.

(2) 提出一个基于雾计算的智能医疗三方认证与密钥协商协议, 基于椭圆曲线 Diffie-Hellman 密钥交换思想构建会话密钥, 实现前向安全性; 会话密钥包含一个长期秘密值, 能够抵抗临时秘密值泄漏攻击; 所提方案实现用户、雾节点、云服务器之间的三方数据安全传输.

(3) 随机预言机模型下安全归约、BAN 逻辑证明与启发式分析显示, 所提方案能实现带隐私保护的双向认证与会话密钥协商, 并且对已知攻击是安全的. 与同类方案的对比分析表明, 所提方案能更好地为智能医疗场景提供安全保护.

1.3 组织架构

本文第 2 节给出预备知识, 第 3 节回顾 Hajian 等人[27]提出的轻量级可穿戴传感设备认证与密钥协商方案; 第 4 节指出 Hajian 等人[27]方案的安全缺陷; 第 5 节回顾 Wu 等人[28]提出的雾辅助无线医疗传感器网络认证方案; 第 6 节指出 Wu 等人[28]方案的安全缺陷; 第 7 节提出一个基于雾计算的智能医疗三方认证与密钥协商协议; 第 8 节给出所提方案的安全分析; 第 9 节给出与同类方案的对比分析; 第 10 节总结. 本文使用的符号如表 1 所示.

表 1 符号表

符号	描述	符号	描述
U_i	用户	$E_{\text{key}}(\cdot)$	AES-128对称加密
ID_i, PW_i, b_i	用户的身份标识, 口令, 生物特征	$D_{\text{key}}(\cdot)$	AES-128对称解密
G_i	智能网关(移动智能设备, 智能家庭中的访问点)	$e(A,B)^C$	双线性配对运算
CSP	云服务器	$\|$	字符串级联操作
F_N	雾节点	$\oplus$	异或运算
S_j	可穿戴传感设备	T_1, T_2, T_3, T_4	时间戳
$\Rightarrow$	通过安全信道传输数据	E_q	椭圆曲线群
$\rightarrow$	通过公共信道传输数据	P	E_q 的生成元
$Rep(\cdot)$	生物特征模糊提取器的确定再生函数	$h(\cdot), h_0(\cdot), h_1(\cdot), h_2(\cdot), h_3(\cdot), h_4(\cdot), h_5(\cdot)$	哈希函数
$Gen(\cdot)$	生物特征模糊提取器的概率生成函数	s, P_{pub}	系统主密钥和公钥

2 预备知识

2.1 椭圆曲线 Diffie-Hellman 问题

椭圆曲线 Diffie-Hellman 问题 (elliptic curve Diffie-Hellman problem, ECDHP): $E_p(a,b)$ 为椭圆曲线上的一个循环群, P 为 $E_p(a,b)$ 的一个生成元, 给定 $E_p(a,b)$ 上的点 rP, sP, tP, 在多项式时间内计算 $rstP$ 是不可行的.

2.2 模糊提取器

用户每次输入的生物特征都存在些微差距, 生物特征模糊提取器用于从用户输入的生物特征中提取生物密

钥, 包含概率生成函数$Gen(\cdot)$以及确定再生函数$Rep(\cdot)$. 概率生成函数$Gen(\cdot)$根据用户所输入的生物特征b_i, 生成一个生物密钥σ_i和一个辅助值θ_i; 当用户再次输入生物特征时, $Rep(\cdot)$函数能够借助辅助值θ_i, 恢复生物密钥σ_i. $Gen(\cdot)$函数在用户注册阶段使用, $Rep(\cdot)$函数在认证阶段使用.

3 Hajian 等人方案回顾

2019 年, Gupta 等人[24]提出一个轻量级的可穿戴传感设备认证与密钥协商方案, 2020 年, Hajian 等人[27]指出 Gupta 等人[24]方案存在安全缺陷: 未实现前向安全性, 不能抵抗离线口令猜测攻击与仿冒攻击, 提出一个新的改进方案. Hajian 等人[27]方案包含 4 个阶段: 系统初始化阶段、注册阶段、认证与密钥协商阶段、口令更新阶段. 口令更新阶段与安全性分析无关, 这里不再赘述. 方案的参与者包括用户、云服务器、可穿戴传感设备. 可穿戴传感设备部署在病人身上, 收集病人的体温、呼吸频率、血压、脉搏等医疗信息, 并将所收集的信息发送给附近的智能网关, 智能网关将数据上传到云服务器, 用户借助智能网关接入网络, 访问云服务器中的数据.

3.1 系统初始化阶段

云服务器 CSP 选取系统主密钥X_{Ser}, 为可穿戴传感设备S_j选取身份标识SID_j, 动态身份标识$TSID_j$, 和长期密钥X_{SD_j}, 将参数<$TSID_j$, X_{SD_j}, SID_j, X_{SD_j}, $h(\cdot)$>存入可穿戴传感设备中, 并将参数<$TSID_j$, X_{SD_j}, SID_j>存进云服务器数据库中. 云服务器为智能网关G_i选取身份标识GID_i, 动态身份标识$TGID_i$, 和长期密钥X_{GD_i}, 智能网关存储参数<$TGID_i$, GID_i, X_{GD_i}, $h(\cdot)$>, 将参数<$TGID_i$, X_{GD_i}, GID_i>存进云服务器数据库中.

3.2 注册阶段

(1) 用户注册阶段

① 用户U_i输入生物特征b_i, 智能网关G_i选择一个随机数r_u, 计算$MI_u = h_1(ID_i \| r_u)$, $MP_u = h_1(PW_i \| b_i \| r_u)$.

② $G_i \Rightarrow CSP: \{MI_u, r_u, ID_i, TGID_i\}$.

③ 云服务器 CSP 收到消息$\{MI_u, r_u, ID_i, TGID_i\}$后, 计算$f_i = h_1(MI_u \| X_{Ser}), x_i = h_1(r_u \| ID_i \| X_{GD_i}), e_i = x_i \oplus f_i$, 将参数$\{MI_u, x_i\}$存进数据库.

④ $CSP \Rightarrow G_i: \{e_i\}$.

⑤ G_i收到消息$\{e_i\}$后, 计算$x_i = h_1(r_u \| ID_i \| X_{GD_i}), f_i = x_i \oplus e_i$, $n_i = MP_u \oplus e_i$, $m_i = r_u \oplus h_1(ID_i \| h_1(PW_i \| b_i))$, 存储参数<$MI_u$, n_i, m_i>. G_i最终存储参数<$TGID_i, GID_i, MI_u$, X_{GD_i}, n_i, $m_i, h(\cdot)$>.

(2) 可穿戴传感设备注册阶段

① 传感设备S_j选取随机数r_j, 计算$MP_j = h_1(SID_j \| TSID_j \| r_j \| T_1)$, $MN_j = h_1(X_{SD_j}, T_1) \oplus r_j$, T_1为当前时间戳.

② $S_j \rightarrow G_i: \{TSID_j, MN_j, MP_j, T_1\}$.

③ G_i收到消息$\{TSID_j, MN_j, MP_j, T_1\}$后, 检查$T_1$的有效性, 若$T_1$有效, 计算$TI_i = h_1(GID_i \| TSID_j \| T_2)$.

④ $G_i \rightarrow CSP: \{TI_i, TGID_i, TSID_j, MN_j, MP_j, T_1, T_2\}$, 其中$T_2$为当前时间戳.

⑤ CSP 收到消息$\{TI_i, TGID_i, TSID_j, MN_j, MP_j, T_1, T_2\}$后, 检查$T_2$的有效性, 若$T_2$有效, 计算$TI_i^* = h_1(GID_i \| TSID_j \| T_2)$, 验证等式$TI_i^* = TI_i$是否成立. 若等式成立, CSP 计算$r_j^* = MN_j \oplus h_1(X_{SD_j}, T_1)$, $MP_j^* = h_1(SID_j \| TSID_j \| r_j^* \| T)$, 验证等式$MP_j^* = MP_j$是否成立. 若等式成立, CSP 计算$f_j = h_1(SID_j \| X_{Ser})$, $x_j = h_1(r_j^* \| X_{SD_j})$, $e_j = f_j \oplus h_1(x_j \| T_3)$, $TI_j = h_1(SID_j \| f_j \| T_3)$, $TI_{Ser} = h_1(GID_i \| f_i \| T_3)$, CSP 将参数$\{x_j\}$存进数据库.

⑥ $CSP \rightarrow G_i: \{e_j, TI_{Ser}, TI_j, T_3\}$.

⑦ G_i收到消息$\{e_j, TI_{Ser}, TI_j, T_3\}$后, 检查$T_3$的有效性, 若$T_3$有效, 计算$TI_{Ser}^* = h_1(GID_i \| f_i \| T_3)$, 验证等式$TI_{Ser}^* = TI_{Ser}$是否成立. 若等式成立, G_i存储$TSID_j$.

⑧ $G_i \rightarrow S_j: \{TI_j, e_j, TGID_i, T_3, T_4\}$, 其中$T_4$为当前时间戳.

⑨ S_j收到消息$\{TI_j, e_j, TGID_i, T_3, T_4\}$后, 检查$T_4$的有效性, 若$T_4$有效, 计算$x_j = h_1(r_j \| X_{SD_j})$, $f_j^* = e_j \oplus h_1(x_j \| T_3)$, $TI_j^* = h_1(SID_j \| f_j^* \| T_3)$, 验证等式$TI_j^* = TI_j$是否成立. 若等式成立, 计算$f_j' = f_j \oplus SID_j$, 存储参数$\{f_j', r_j\}$. S_j最终存储参数<$TSID_j, X_{SD_j}, SID_j, f_j', r_j$>.

3.3 认证与密钥协商阶段

(1) 用户 U_i 输入身份标识 ID_i, 口令 PW_i, 生物特征 b_i, 智能网关 G_i, 计算 $r_u^* = m_i \oplus h_1(ID_i \| h_1(PW_i \| b_i))$, $MI_u^* = h_1(ID_i \| r_u^*)$, 检查等式 $MI_u^* = MI_u$ 是否成立. 若等式成立, 计算 $MP_u^* = h_1(PW_i \| b_i \| r_u^*)$, $x_i^* = h_1(r_u^* \| ID_i \| X_{GD_i})$, $f_i^* = n_i \oplus x_i^* \oplus MP_u^*$, $MID_u = h_1(f_i^* \| MI_u \| T_1)$.

(2) $G_i \to S_j : \{MID_u, TGID_i, T_1\}$.

(3) 可穿戴传感设备 S_j 收到消息 $\{MID_u, TGID_i, T_1\}$ 后, 检查 T_1 的有效性, 若 T_1 有效, 计算 $f_j = f_j' \oplus SID_j$, $A_j = h_1(MID_u \| X_{SD_j} \| f_j \| T_1)$, $x_j = h_1(r_j \| X_{SD_j})$, 选取随机数 k_j, 计算 $v_j = h_1(f_j \| x_j \| T_1)$, $Z_j = k_j \oplus h_1(v_j \| TSID_j \| T_2)$.

(4) $S_j \to G_i : \{TSID_j, A_j, Z_j, T\}$.

(5) G_i 收到消息 $\{TSID_j, A_j, Z_j, T_2\}$ 后, 检查 T_2 的有效性, 若有效, 计算 $M_1 = h_1(TGID_i \| MID_u \| X_{GD_i} \| TSID_j \| T_3)$, 存储参数 Z_j.

(6) $G_i \to CSP : \{TGID_i, TSID_j, M_1, A_j, T_1, T_3\}$.

(7) CSP 收到消息 $\{TGID_i, TSID_j, M_1, A_j, T_1, T_3\}$ 后, 检查 T_3 的有效性, 若 T_3 有效, 计算 $MID_u = h_1(f_i \| MI_u \| T_1)$, $A_j^* = h_1(MID_u \| X_{SD_j} \| f_j \| T_1)$, $M_1^* = h_1(TGID_i \| MID_u \| X_{GD_i} \| TSID_j \| T_3)$, 验证等式 $A_j^* = A_j$ 与 $M_1^* = M_1$ 是否成立.若等式成立, CSP 计算 $v_j = h_1(f_j \| x_j \| T)$, $M_2 = h_1(f_i \| X_{GD_i} \| TSID_j \| T_4)$, $M_3 = v_j \oplus M_2$, 为 S_j 计算新的动态身份标识 $TSID_j^{\text{new}} = h_1(v_j \| TSID_j \| T_4)$, 在数据库中将 $TSID_j$ 更新为 $TSID_j^{\text{new}}$, 计算 $M_4 = h_1(TSID_j^{\text{new}} \| X_{SD_j} \| v_j \| TGID_i \| T_4)$.

(8) $CSP \to G_i : \{M_2, M_3, M_4, T_4\}$.

(9) G_i 收到消息 $\{M_2, M_3, M_4, T_4\}$ 后, 检查 T_4 的有效性, 若 T_4 有效, 计算 $M_2^* = h_1(f_i^* \| X_{GD_i} \| TSID_j \| T_4)$, 验证等式 $M_2^* = M_2$ 是否成立. 若等式成立, G_i 计算 $v_j = M_3 \oplus M_2$, $k_j = Z_j \oplus h_1(v_j \| TSID_j \| T_2)$, $TSID_j^{\text{new}} = h_1(v_j \| TSID_j \| T_4)$, 选取随机数 k_i, 计算 $M_5 = k_i \oplus h_1(v_j \| T_5)$, $sk = h_1(k_i \| k_j)$, $M_6 = h_1(sk \| TSID_j^{\text{new}} \| TGID_i \| T_5)$.

(10) $G_i \to S_j : \{M_4, M_5, M_6, T_4, T_5\}$.

(11) S_j 收到消息 $\{M_4, M_5, M_6, T_4, T_5\}$ 后, 检查 T_5 的有效性, 若 T_5 有效, 计算 $TSID_j^{\text{new}} = h_1(v_j \| TSID_j \| T_4)$, $M_4^* = h_1(TSID_j^{\text{new}} \| X_{SD_j} \| v_j \| TGID_i \| T_4)$, $k_i = M_5 \oplus h_1(v_j \| T_5)$, $sk = h_1(k_i \| k_j)$, $M_6^* = h_1(sk \| TSID_j^{\text{new}} \| TGID_i \| T_5)$, 验证等式 $M_4^* = M_4$ 与 $M_6^* = M_6$ 是否成立. 若等式成立, 表明用户和可穿戴设备成功协商会话密钥 sk.

4 Hajian 等人方案安全性分析

Hajian 等人在文献 [27] 中指出 Gupta 等人[24]方案存在安全缺陷, 例如, 未实现前向安全性, 不能抵抗离线口令猜测攻击与仿冒攻击. 参照 Wang 等人多因素协议攻击者模型[29,30]对 Hajian 等人[27]方案进行安全分析, 发现 Hajian 等人[27]方案同样未能实现前向安全性, 并且遭受设备捕获攻击、会话密钥泄漏攻击、验证表丢失攻击、拒绝服务攻击.

4.1 前向安全性

前向安全性评估在攻击者获得系统长期密钥的情况下, 系统所建立会话密钥的安全性. 未能满足前向安全性的方案, 在系统被攻破时, 将泄漏系统内全部的会话密钥. 可穿戴传感设备与用户所交互的数据与病人的身体健康密切相关, 方案应能够满足前向安全性.

攻击者获取服务器密钥 X_{Ser} 与服务器数据库中保存的参数 x_j 后, 通过执行以下步骤可计算出用户和可穿戴传感设备所协商的会话密钥:

(1) 从公共信道截获消息 $\{TSID_j, A_j, Z_j, T_2\}$ 与 $\{M_4, M_5, M_6, T_4, T_5\}$.

(2) 计算 $f_j = h_1(SID_j \| X_{Ser})$, $v_j = h_1(f_j \| x_j \| T_1)$, $k_j = Z_j \oplus h_1(v_j \| TSID_j \| T_2)$, $k_i = M_5 \oplus h_1(v_j \| T_5)$.

(3) 计算会话密钥 $sk = h_1(k_i \| k_j)$.

4.2 传感设备捕获攻击

可穿戴传感设备通常计算能力与存储能力都十分受限, 相比服务器、手机等智能终端将更容易攻破. 在现实

生活中, 传感设备被成功攻破的例子层出不穷, 由此可见, 传感设备捕获攻击[31]是一种十分现实的攻击场景. 在遭受传感设备捕获攻击后, 可穿戴传感设备密钥被泄漏会影响其他通信方的安全性. 在 Hajian 等人[27]方案中, 攻击者借助所捕获可穿戴传感设备的密钥$<TSID_j, X_{SD_j}, SID_j, f'_j, r_j>$, 能够计算出可穿戴传感设备和用户协商的全部会话密钥, 进而恢复通信数据.

(1) 攻击者攻破可穿戴传感设备S_j后, 得到存储的参数$<TSID_j, X_{SD_j}, SID_j, f'_j, r_j>$, 计算$f_j = f'_j \oplus SID_j$, 成功恢复可穿戴传感设备的密钥$f_j$.

(2) 从公共信道截获消息$<TSID_j, A_j, Z_j, T_2>$与$<M_4, M_5, M_6, T_4, T_5>$.

(3) 计算$x_j = h_1(r_j \| X_{SD_j})$, $v_j = h_1(f_j \| x_j \| T_1)$, $k_j = Z_j \oplus h_1(v_j \| TSID_j \| T_2)$, $k_i = M_5 \oplus h_1(v_j \| T_5)$.

(4) 计算会话密钥$sk = h_1(k_i \| k_j)$.

4.3 会话密钥泄漏攻击

攻击者可根据公共信道截获的消息恢复出会话密钥, 攻击步骤如下:

(1) 攻击者从公共信道截获消息$\{TSID_j, A_j, Z_j, T_2\}$, $\{M_2, M_3, M_4, T_4\}$, $\{M_4, M_5, M_6, T_4, T_5\}$.

(2) 攻击者计算$v_j = M_3 \oplus M_2$, $k_j = Z_j \oplus h_1(v_j \| TSID_j \| T_2)$, $k_i = M_5 \oplus h_1(v_j \| T_5)$, $sk = h_1(k_i \| k_j)$.

4.4 验证表丢失攻击

验证表丢失攻击是一种经典的攻击. 攻击者通过对服务器发起攻击, 获取服务器数据库中存储的部分甚至全部数据. 在 Hajian 等人[27]方案中, 攻击者能够借助获取的服务器数据库中的参数, 恢复可穿戴传感设备的密钥, 进而利用所恢复密钥发起用户仿冒攻击、拒绝服务攻击.

(1) 攻击者获取服务器中数据库存储的参数$<TSID_j, X_{SD_j}, SID_j, x_j>$.

(2) 在传感设备注册阶段, 从公共信道截获消息$<e_j, TI_{Ser}, TI_j, T_3>$.

(3) 计算可穿戴传感设备的密钥$f_j = e_j \oplus h_1(x_j \| T_3)$.

4.5 仿冒攻击

得到可穿戴传感设备S_j的全部参数$<TSID_j, X_{SD_j}, SID_j, x_j, f_j>$后, 攻击者所具备的能力将与该可穿戴传感设备没有任何差别. 通过以下步骤, 攻击者可以伪装成S_j与用户和云服务器完成相互认证与会话密钥协商.

(1) 从公共信道截获G_i发送给S_j的消息$\{MID_u, TGID_i, T_1\}$.

(2) 执行认证与密钥协商阶段的步骤 (3), 将消息$\{TSID_j, A_j, Z_j, T_2\}$发送给$G_i$.

(3) 截获G_i发送给S_j的消息$\{M_4, M_5, M_6, T_4, T_5\}$.

(4) S_j检查T_5的有效性, 若T_5有效, 计算$TSID_j^{new} = h_1(v_j \| TSID_j \| T_4)$, $M_4^* = h_1(TSID_j^{new} \| X_{SD_j} \| v_j \| TGID_i \| T_4)$, $k_i = M_5 \oplus h_1(v_j \| T_5)$, $sk = h_1(k_i \| k_j)$, $M_6^* = h_1(sk \| TSID_j^{new} \| TGID_i \| T_5)$, 验证等式$M_4^* = M_4$与$M_6^* = M_6$是否成立. 若等式成立, 则表明攻击者成功地伪装成S_j与用户协商得到会话密钥sk.

4.6 拒绝服务攻击

拒绝服务攻击是一种常见攻击, 攻击者通常通过消息洪泛, 或令用户与服务器失去同步, 使服务器拒绝用户访问. 在 Hajian 等人[27]方案中, 攻击者在获得可穿戴传感设备S_j的全部参数$<TSID_j, X_{SD_j}, SID_j, x_j, f_j>$后, 伪装成$S_j$向云服务器发送消息, 云服务器为$S_j$生成一个新动态身份标识$TSID_j^{new}$, 并将数据库中的$TSID_j$更新为$TSID_j^{new}$. 当用户再次访问$S_j$时, 由于在云服务器数据库中找不到$TSID_j$的对应项, 云服务器认为$S_j$是非法的, 从而导致$S_j$无法访问.

(1) 从公共信道截获G_i发送给S_j的消息$\{MID_u, TGID_i, T_1\}$.

(2) 执行认证与密钥协商阶段的步骤 (3), 将消息$\{TSID_j, A_j, Z_j, T_2\}$发送给$G_i$.

(3) G_i执行认证与密钥协商阶段的步骤 (5) 和 (6); CSP执行认证与密钥协商阶段的步骤 (7) 和 (8), 在数据库中将$TSID_j$更新为$TSID_j^{new}$; G_i执行认证与密钥协商阶段的步骤 (9) 和 (10).

可穿戴传感设备S_j中存储的动态身份标识为$TSID_j$, 而云服务器数据库中已将旧的动态身份标识$TSID_j$更新为新的动态身份标识$TSID_j^{new}$, 云服务器认为可穿戴传感设备S_j是非法的, S_j所收集数据将无法访问.

Hajian 等人[27]方案未能构建安全会话密钥的原因在于方案中利用参数v_j传递随机数k_j, 利用随机数k_j传递随机数k_i. 由于 *CSP* 向用户传递参数v_j时, 利用M_2异或加密v_j, 得到参数M_3, 并将M_2与M_3一起传递给用户, 这势必造成参数v_j的泄漏, 从而影响会话密钥安全性. 这说明在会话密钥协商过程中, 随机数的安全传递是个关键的问题, Diffie-Hellman 密钥交换是解决该问题的一个很好选择. Hajian 等人[27]方案遭受其他攻击的原因在于, *CSP* 端维护一个验证表, 攻击者利用验证表中的数据能够恢复可穿戴传感设备的密钥f_j, 协议失效本质原因在于验证表中存有导致密钥泄漏的参数.

5 Wu 等人协议回顾

2019 年, Jia 等人[25]提出一个基于双线性对的雾辅助智能医疗传感器网络认证方案, 2021 年, Wu 等人[28]指出 Jia 等人[25]方案存在安全缺陷, 提出一个新的改进方案. Wu 等人[28]方案包含 3 个阶段: 用户注册阶段、雾节点注册阶段、认证与密钥协商阶段. 方案的参与者包括用户、云服务器、雾节点. 系统初始化时, *CSP* 选取系统主密钥 s, 计算公钥 $P_{\text{pub}} = sP$.

5.1 用户注册阶段

(1) 用户 U_i 选取身份标识ID_i与口令 PW_i, 选取一个随机数 r_i, 计算$RID_i = h_1(ID_i \| PW_i) \oplus r_i$.

(2) $U_i \Rightarrow CSP: \{ID_i, RID_i\}$.

(3) 云服务器收到消息 $\{ID_i, RID_i\}$ 后, *CSP* 选取随机数x_i, 计算$q_i = h_2(ID_i \| s \| x_i)$, 计算$R_i = q_i \oplus RID_i$, $D_i = h_2(q_i \| ID_i) \oplus RID_i$, 将参数$\{ID_i, x_i\}$存进数据库, 将参数$\{R_i, D_i\}$ 存进智能卡.

(4) $CSP \Rightarrow U_i$: 智能卡.

(5) U_i 收到智能卡后, 计算$G_i = R_i \oplus r_i$, $V_i = D_i \oplus r_i$, 从智能卡中删除参数R_i, D_i, 将参数G_i, V_i存进智能卡.

5.2 雾节点注册阶段

(1) 雾节点 F_N 选取身份标识ID_j, 将消息$\{ID_j\}$通过安全信道发送给 *CSP*.

(2) *CSP* 收到消息$\{ID_j\}$后, 选取随机数$y_j \in Z_p^*$, 计算$g_j = h_2(ID_j \| s \| y_j)$. *CSP* 将参数$\{ID_j, y_j\}$存进数据库.

(3) $CSP \Rightarrow F_N: \{g_j\}$.

5.3 认证与密钥协商阶段

(1) 用户 U_i 输入身份标识ID_i 与口令 PW_i, 智能卡计算$q_i = G_i \oplus h_1(ID_i \| PW_i)$, $V_i^* = h_2(q_i \| ID_i) \oplus h_1(ID_i \| PW_i)$, 验证等式 $V_i^* = V_i$ 是否成立. 若等式成立, U_i 选取随机数$a \in Z_p^*$, 计算$v_u = a \cdot q_i$, $A = v_u P$, $C = v_u \cdot P_{\text{pub}}$, $PID_i = ID_i \oplus h_0(C)$, $N_i = h_3(C \| q_i \| A \| ID_i \| ID_j \| T_1)$, T_1 为当前时间戳.

(2) $U_i \rightarrow F_N: \{A, PID_i, N_i, T_1\}$.

(3) 雾节点 F_N 收到消息$\{A, PID_i, N_i, T_1\}$ 后, 验证T_1 的有效性, 若T_1 有效, 选取随机数$b \in Z_p^*$, 计算$v_f = b \cdot g_j$, $B = v_f \cdot P$, $D = v_f \cdot P_{\text{pub}}$, $PID_j = ID_j \oplus h_0(D)$, $L_j = h_3(C \| g_j \| A \| PID_j \| ID_j \| T_2)$, T_2 为当前时间戳.

(4) $F_N \rightarrow CSP: \{A, B, PID_i, PID_j, N_i, L_j, T_1, T_2\}$.

(5) *CSP* 收到消息 $\{A, B, PID_i, PID_j, N_i, L_j, T_1, T_2\}$ 后, 验证T_1, T_2 的有效性, 若T_1, T_2 有效, 计算$C = s \cdot A$, $ID_i = PID_i \oplus h_0(C)$, 从数据库中提取 $\{ID_i, x_i\}$, 计算 $q_i = h_2(ID_i \| s \| x_i)$, $N_i^* = h_3(C \| q_i \| A \| ID_i \| ID_j \| T)$, 验证等式$N_i^* = N_i$ 是否成立. 计算$D = s \cdot B$, $ID_j = PID_j \oplus h_0(D)$, 从数据库中找到$\{ID_j, y_j\}$, 计算 $g_j = h_2(ID_j \| s \| y_j)$, $L_j^* = h_3(C \| g_j \| A \| PID_j \| ID_j \| T_2)$, 验证等式$L_j^* = L_j$ 是否成立. 若等式成立, *CSP* 选取随机数$c \in Z_p^*$, 计算$z_c = h_2(y_j \| s \| x_i)$, $v_c = c \cdot z_c$, $E = v_c P$, $F_i = h_4(A \| B \| E \| C \| ID_i \| T_3)$, $F_j = h_4(A \| B \| E \| D \| ID_j \| T_3)$, $K = e(A, B)^{v_c}$, $sk = h_5(K \| A \| B \| E)$.

(6) $CSP \rightarrow F_N: \{E, F_i, F_j, T_3\}$.

(7) 雾节点 F_N 收到消息$\{E, F_i, F_j, T_3\}$ 后, 验证T_3的有效性, 若T_3有效, 计算$F_j^* = h_4(A \| B \| E \| D \| ID_j \| T_3)$, 验证等式$F_j^* = F_j$是否成立. 若等式成立, 计算$K = e(A, E)^{v_f}$, $sk = h_5(K \| A \| B \| E)$.

(8) $F_N \rightarrow U_i: \{B, E, F_i, T_3\}$.

(9) 用户 U_i 收到消息$\{B,E,F_i,T_3\}$后, 验证T_3的有效性, 计算$F_i^* = h_4(A \| B \| E \| C \| ID_i \| T_3)$, 验证等式$F_i^* = F_i$是否成立. 若等式成立, 计算$K = e(B,E)^{v_u}$, $sk = h_5(K \| A \| B \| E)$.

6 Wu 等人方案安全性分析

6.1 离线口令猜测攻击

离线口令猜测攻击是指, 在智能卡非抗篡改假设下, 攻击者在获得用户智能卡后, 通过离线遍历口令字典确定用户口令. 用户身份标识受限于一个有限空间, 用户通常不会像保存口令一样安全的保存用户口令, 因此一般假设攻击者能够在多项式时间内遍历用户身份标识和口令字典. 攻击者获取用户 U_i 的智能卡参数$\{G_i,V_i\}$, 通过以下步骤猜测用户 U_i 的口令:

(1) 从用户身份标识字典空间选取ID_i^*, 从口令字典空间选取PW_i^*.

(2) 计算$q_i^* = G_i \oplus h_1(ID_i^* \| PW_i^*)$, $V_i^* = h_2(q_i^* \| ID_i^*) \oplus h_1(ID_i^* \| PW_i^*) = h_2(G_i \oplus h_1(ID_i^* \| PW_i^*) \| ID_i^*) \oplus h_1(ID_i^* \| PW_i^*)$, 验证等式$V_i^* = V_i$是否成立, 若等式成立, 表明$(ID_i^*, PW_i^*)$为用户正确的身份标识与口令.

(3) 若$V_i^* \neq V_i$, 重复执行步骤 (1) 和 (2), 直到找到正确的(ID_i^*, PW_i^*).

Wu 等人[28]协议未能抵抗离线字典猜测攻击的原因在于, 智能卡中存在验证值V_i, 攻击者可以利用该验证值验证所猜测口令的正确性, 找到用户正确口令.

6.2 仿冒攻击

攻击者通过离线口令猜测攻击得到用户身份标识与口令后, 攻击者所具备的能力与用户 U_i 没有任何差别, 攻击者通过以下步骤伪装成用户 U_i, 与雾节点以及云服务器完成相互认证及会话密钥协商.

(1) 选取随机数$a \in Z_p^*$, 计算 $v_u = a \cdot q_i$, $A = v_u \cdot P$, $C = v_u \cdot P_{\text{pub}}$, $PID_i = ID_i \oplus h_0(C)$, $N_i = h_3(C \| q_i \| A \| ID_i \| ID_j \| T_1)$, 其中$T_1$为当前时间戳, 将消息$\{A, PID_i, N_i, T_1\}$通过公共信道发送给雾节点 F_N.

(2) 雾节点 F_N 与 CSP 执行认证与密钥协商阶段的步骤 (3)–(8).

(3) 从公共信道截获消息$\{B,E,F_i,T_3\}$.

(4) 验证T_3的有效性, 计算$F_i^* = h_4(A \| B \| E \| C \| ID_i \| T_3)$, 验证等式$F_i^* = F_i$是否成立. 若等式成立, 计算$K = e(B,E)^{v_u}$, $sk = h_5(K \| A \| B \| E)$.

Wu 等人[28]方案存在安全缺陷的根本原因在于智能卡中存在验证值V_i. 在认证协议中, 智能卡中往往存在一个验证用户输入口令正确性的验证值, 但是该验证值的存在, 容易导致离线口令猜测攻击, 为解决该问题, 可以采用 Wang 等人[32]提出模糊验证技术, 这一技术很好地解决了因为本地验证引起的离线口令猜测问题.

7 提出新的协议

本节提出一个基于雾计算的智能医疗三方认证与密钥协商方案. 方案的参与者包括用户、雾节点、云服务器, 所提方案实现用户、雾节点、云服务器三方相互认证与会话密钥协商. 所提方案包含以下 7 个阶段.

7.1 系统初始化阶段

输入安全参数 l, 云服务器 CSP 选取有限域F_p上的一个椭圆曲线群$E_p(a,b)$, 其中 p 为大质数. P 为$E_p(a,b)$的一个生成元. CSP 选取系统主密钥 s, 计算公钥$P_{\text{pub}} = sP$, 选取一个安全的哈希函数$h_1(\cdot)$, 选取对称密码 AES-128 算法$E_k(\cdot)/D_k(\cdot)$.

7.2 用户注册阶段

(1) 用户 U_i 选取身份标识ID_i与口令PW_i, 输入生物特征b_i, 计算$(\sigma_i,\theta_i) = Gen(b_i)$, $RID_i = h_1(ID_i \| PW_i \| \sigma_i)$.

(2) $U_i \Rightarrow CSP: \{ID_i, RID_i\}$.

(3) CSP 收到消息$\{ID_i, RID_i\}$后, 选取随机数 x_i, x_i为模糊验证因子, 用于检测用户获得智能卡后的在线猜测攻击. CSP 计算$A_i = h_1(ID_i \| s \| x_i)$, $R_i = A_i \oplus RID_i$. CSP 将参数$\{R_i, x_i\}$存进智能卡, 将参数$\{ID_i, x_i, cou = 0\}$存进数据库.

(4) $CSP \Rightarrow U_i$: 智能卡.

(5) U_i 收到智能卡后, 计算 $V_i = h(ID_i \| PW_i \| \sigma_i) \mod n$, 其中 n 为满足 $2^8 \leqslant n \leqslant 2^{10}$ 的一个整数, 将参数 $\{V_i, \theta_i\}$ 存进智能卡.

7.3 雾节点注册阶段

(1) 雾节点 F_N 选取身份标识 ID_j, 将 $\{ID_j\}$ 通过安全信道发送给 CSP.

(2) CSP 收到 $\{ID_j\}$ 后, 选取随机数 $y_j \in Z_p^*$, 计算 $k_j = h_1(ID_j \| s \| y_j)$. CSP 将参数 $\{ID_j, y_j\}$ 存进数据库.

(3) $CSP \Rightarrow F_N : \{k_j\}$. CSP 通过物理注入的方式将密钥写入雾节点.

7.4 认证与密钥协商阶段

所提方案的认证与密钥协商阶段如图 1 所示.

(1) 用户 U_i 输入身份标识 ID_i 与口令 PW_i, 输入生物特征 b_i, 计算 $\sigma_i = Rep(b_i, \theta_i)$, $RID_i = h_1(ID_i \| PW_i \| \sigma_i)$, $V_i^* = RID_i \mod n$, 验证等式 $V_i^* = V_i$ 是否成立. 若等式成立, 选取随机数 $r_1 \in Z_p^*$, 计算 $B_i = r_1 P$, $C_i = r_1 \cdot P_{\text{pub}}$, $F_i = E_{C_i}(ID_i \| x_i)$, $A_i = R_i \oplus RID_i$, $G_i = h_1(A_i \| B_i \| F_i \| T_1)$, 其中 T_1 为当前时间戳.

(2) $U_i \rightarrow F_N : \{B_i, F_i, G_i, T_1\}$.

(3) 雾节点 F_N 收到消息 $\{B_i, F_i, G_i, T_1\}$ 后, 验证 T_1 的有效性, 若 T_1 有效, 选取随机数 r_2, 计算 $L_i = r_2 P$, $N_i = r_2 \cdot P_{\text{pub}}$, $O_i = E_{N_i}(ID_j \| r_2 \cdot B_i)$, $M_i = h_1(k_j \| L_i \| O_i \| G_i \| T_2)$, 其中 T_2 为当前时间戳.

(4) $F_N \rightarrow CSP : \{B_i, F_i, G_i, T_1, L_i, O_i, M_i, T_2\}$.

(5) CSP 收到消息 $\{B_i, F_i, G_i, T_1, L_i, O_i, M_i, T_2\}$ 后, 验证 T_2 的有效性, 若 T_2 有效, 计算 $N_i = s \cdot L_i$, $(ID_j \| r_2 B_i) = D_{N_i}(O_i)$. 根据 ID_j 在数据库中检索 $\{ID_j, y_j\}$, 计算 $k_j = h_1(ID_j \| s \| y_j)$, $M_i^* = h_1(k_j \| L_i \| O_i \| G_i \| T_2)$, 验证等式 $M_i^* = M_i$ 是否成立. 若等式成立, CSP 成功认证雾节点 F_N, 执行下一步骤.

(6) CSP 计算 $C_i = s \cdot B_i$, $(ID_j \| x_i^*) = D_{C_i}(F_i)$. 根据 ID_j 在数据库中找到 $\{ID_j, x_i\}$, 验证等式 $x_i^* = x_i$ 是否成立. 若等式成立, 计算 $A_i = h_1(ID_i \| s \| x_i)$, $G_i^* = h_1(A_i \| B_i \| F_i \| T_1)$, 验证等式 $G_i^* = G_i$ 是否成立. 若等式不成立, 表明用户智能卡很可能被攻击者捕获, 执行 $cou = cou + 1$. 当 $cou \geqslant 10$ 时, 智能卡将被挂起. 若 $G_i^* = G_i$, CSP 成功认证用户 U_i, 执行下一步骤.

(7) CSP 选取随机数 r_3, 计算会话密钥 $sk = h_1(h_1(A_i \| C_i) \| h_1(r_3 \cdot r_2 B_i))$, 计算 $Q_i = E_{k_j}(r_3 \cdot B_i \| h_1(A_i \| C_i))$, $Y_i = E_{C_i}(r_3 \cdot L_i)$, $Z_i = h_1(Y_i \| A_i)$, $W_i = h_1(k_j \| Q_i \| Y_i \| Z_i)$.

(8) $CSP \rightarrow F_N : \{Q_i, W_i, Y_i, Z_i\}$.

(9) F_N 收到消息 $\{Q_i, W_i, Y_i, Z_i\}$ 后, 计算 $W_i^* = h_1(k_j \| Q_i \| Y_i \| Z_i)$, 验证等式 $W_i^* = W_i$ 是否成立, 若等式成立, 计算 $(r_3 B_i \| h_1(A_i \| C_i)) = D_{k_j}(Q_i)$, $sk = h_1(h_1(A_i \| C_i) \| h_1(r_2 \cdot r_3 B_i))$.

(10) $F_N \rightarrow U_i : \{Y_i, Z_i\}$.

(11) U_i 收到消息 $\{Y_i, Z_i\}$ 后, 计算 $Z_i^* = h_1(Y_i \| A_i)$, 验证等式 $Z_i^* = Z_i$ 是否成立. 若等式成立, 计算 $r_3 L_i = D_{C_i}(Y_i)$, $sk = h_1(h_1(A_i \| C_i) \| h_1(r_1 \cdot r_3 L_i))$.

7.5 用户口令与生物特征更新阶段

用户通过以下步骤在本地更新口令与生物特征.

(1) 用户 U_i 输入身份标识 ID_i, 口令 PW_i, 生物特征 b_i, 智能卡计算 $(\sigma_i, \theta_i) = Gen(b_i)$, $RID_i = h_1(ID_i \| PW_i \| \sigma_i)$, $V_i^* = RID_i \mod n$, 验证等式 $V_i^* = V_i$ 是否成立. 若等式成立, 允许用户输入新的口令和生物特征.

(2) 收到用户新的口令 PW_i' 和生物特征 b_i' 后, 智能卡计算 $(\sigma_i', \theta_i') = Gen(b_i')$, $RID_i' = h_1(ID_i \| PW_i' \| \sigma_i')$, $V_i' = RID_i' \mod n$, $R_i' = R_i \oplus RID_i \oplus RID_i'$. 智能卡存储参数 $\{R_i', x_i, V_i', \theta_i'\}$.

7.6 用户重注册阶段

当云服务器检测到针对用户 U_i 的在线口令猜测攻击, 将挂起 U_i 的智能卡, 此时, U_i 执行用户重注册, 获取一

张新的智能卡.

(1) 用户 U_i 输入身份标识 ID_i、口令 PW_i、生物特征 b_i, 计算 $(\sigma_i,\theta_i)=Gen(b_i)$, $RID_i=h_1(ID_i \| PW_i \| \sigma_i)$.

(2) $U_i \Rightarrow CSP:\{ID_i,RID_i\}$.

(3) 收到消息 $\{ID_i,RID_i\}$ 后, CSP 选取随机数 x_i, 计算 $A_i=h(ID_i \| s \| x_i)$, $R_i=A_i \oplus RID_i$. CSP 将参数 $\{R_i,x_i\}$ 存进智能卡, 将参数 $\{ID_i,x_i,cou=0\}$ 存进数据库.

(4) $CSP \Rightarrow U_i$:智能卡.

图 1 所提方案认证与密钥协商阶段

(5) 收到智能卡后, U_i 计算 $V_i = h(ID_i \| PW_i \| \sigma_i) \mod n$, 将参数 $\{V_i, \theta_i\}$ 存进智能卡.

CSP 基于随机数 x_i 生成认证秘密值 A_i, 用户重注册时无需改变用户身份标识, 便能为用户生成新的智能卡参数.

7.7 动态雾节点增加阶段

(1) 雾节点 F_N 选取身份标识 ID_j, 将 $\{ID_j\}$ 通过安全信道发送给 *CSP*.

(2) 收到 $\{ID_j\}$ 后, *CSP* 选取随机数 $y_j \in Z_p^*$, 计算 $k_j = h(ID_j \| s \| y_j)$. *CSP* 将参数 $\{ID_j, y_j\}$ 存进数据库.

(3) $CSP \Rightarrow F_N : \{k_j\}$.

8 安全性证明

基于 Bellare 等人提出的认证协议安全模型[33], 首先提出雾架构三因子认证方案安全模型, 在该模型下证明所提方案的安全性. 并运用启发式分析证明所提方案对已知攻击是安全的.

8.1 安全模型

● 参与者. 方案的参与者包括云服务器 *CSP*、雾节点 F_j 和用户 U_i, 每个参与者包含多个实例, 即 CSP^a, F_j^a, U_i^a.

● 查询. 攻击者 $\mathcal{A}$ 通过以下查询与参与者进行交互, 从而模拟攻击者的能力.

Execute (CSP^a, F_j^a, U_i^a). 模拟窃听攻击, 预言机将公开信道传送的消息副本返回给 $\mathcal{A}$.

Send $(CSP^a / F_j^a / U_i^a, m)$. 此查询模拟主动攻击, 攻击者 $\mathcal{A}$ 向实例 $CS^a / S_j^a / U_i^a$ 发送消息 *m*, 实例按照协议处理消息 *m*, 并返回一个响应消息.

Reveal (F_j^a, U_i^a). 若实例 F_j^a 与 U_i^a 生成一个会话密钥, 将 F_j^a 与 U_i^a 生成的会话密钥返回给攻击者, 否则返回 $\perp$.

Corrupt (U_i^a, ϕ). 该预言机揭示用户的一种或两种认证信息.

$\phi = 1$ 时, 返回用户智能卡;

$\phi = 2$ 时, 返回用户口令;

$\phi = 3$ 时, 返回用户生物特征.

Corrupt (CSP^a, F_j^a). 模拟前向安全性, 将云服务器的密钥或雾节点密钥返回给攻击者.

Test (F_j^a, U_i^a). 该查询最多运行一次. 如果实例 F_j^a 与 U_i^a 是新鲜的 (参阅下文) 并且生成会话密钥 *SK*, 预言机投掷硬币 b, 若 $b = 1$, 输出会话密钥 *SK*; 若 $b = 0$, 输出会话密钥的一个等长随机字符串.

● 新鲜性. 若实例 S_j^a / U_i^a 是新鲜的, 那么表示:

① S_j^a / U_i^a 实例正确运行, 且生成会话密钥 *SK*.

② 攻击者未对实例 S_j^a / U_i^a 及其伙伴进行过 *Corrupt* (S_j^a / CS^a) 和 *Reveal* (S_j^a / U_i^a) 查询.

● 语义安全性. 攻击者通过进行上述查询, 推断 *Test*$((S_j^a / U_i^a))$ 查询中 b 的值为 b', 攻击者攻破认证方案语义安全性的优势定义为:

$$Adv_P^{ake}(\mathcal{A}) = 2Pr(b' = b) - 1 \tag{1}$$

若 $Adv_P^{ake}(\mathcal{A})$ 是可忽略的, 方案具有语义安全性.

8.2 安全证明

定理 1. 口令空间 D_{PW} 服从 Zipf 分布[27]. 假设攻击者 $\mathcal{A}$ 在多项式时间内可进行 q_e 次 Execute 查询, q_h 次哈希查询, q_s 次 Send 查询, q_f 次模糊提取器的概率生成函数查询和 q_ε 次对称加密/解密查询, 则有:

$$Adv_P^{ake}(\mathcal{A}) \leqslant 2C' * {q_s}^{s'} + \frac{(q_s + q_e)^2}{p} + \frac{6q_s + q_h^2}{2^{l_1}} + \frac{2q_s + q_f^2}{2^{l_2}} + \frac{q_\varepsilon^2}{2^{l_3}} + 2q_h Adv_P^{\mathrm{ECDHP}} \tag{2}$$

其中, l_1, l_2, l_3 分别是哈希函数、概率生成函数、对称加密输出的位长度. Adv_P^{ECDHP} 为攻击者 $\mathcal{A}$ 解决 ECDHP 的优势. 以 Tianya 口令数据集[34]为例, $|D_{PW}| \approx 13$ million, $s' = 0.155478$, $C' = 0.062239$.

证明: 为证明定理 1, 定义一系列游戏 $\Phi_i\ (0 \leqslant i \leqslant 6)$. $Pr[\chi_i]$ 表示攻击者 $\mathcal{A}$ 在游戏 G_i 中成功猜测 b 的值的概率.

Φ_0: 该游戏模拟攻击者对真实协议的攻击, 因此有:

$$Adv_P^{ake}(\mathcal{A}) = 2(Pr[\chi_0]) - 1 \tag{3}$$

Φ_1: 该游戏使用哈希列表Λ_H和对称加密/解密列表Λ_S来模拟哈希预言机和对称加密/解密预言机. 收到哈希查询$H_1(a)$时, 首先查找列表Λ_H, 若Λ_H包含有关a的一条记录(a,b), 返回b; 否则, 选取随机数b作为a的哈希值, 并将记录(a,b)添加到列表Λ_H. 收到加密查询$E_k(\alpha)$时, 首先查找列表Λ_S, 若Λ_S包含一条相关的记录(k,α,β), 返回β; 否则, 选取随机字符串β作为a的加密结果 (密文), 并将记录(k,α,β)添加到列表Λ_S. 收到解密查询$D_k(\beta)$时, 首先查找列表Λ_S, 若Λ_S包含一条相关的记录(k,α,β), 返回α; 否则, 选取随机字符串α作为β的解密结果 (明文), 并将记录(k,α,β)添加到列表Λ_ε. 该游戏与游戏Φ_0是不可区分的, 因此有:

$$Pr[\chi_0] - Pr[\chi_1] = 0 \tag{4}$$

Φ_2: 该游戏去除一些碰撞的发生, 以下情形发生时, 游戏终止:

情形 1. 哈希函数或模糊提取器概率生成函数的输出发生碰撞;

情形 2. 对称加密的输出 (密文) 发生碰撞, 其概率为$q_\varepsilon^2/2^{l_3+1}$;

情形 3. 生成的消息发生碰撞.

根据生日悖论原理, 得到:

$$\left|Pr[\chi_1] - Pr[\chi_2]\right| \leqslant \frac{q_h^2}{2^{l_1+1}} + \frac{q_f^2}{2^{l_2+1}} + \frac{q_\varepsilon^2}{2^{l_3+1}} + \frac{(q_s+q_e)^2}{2p} \tag{5}$$

Φ_3: 如果攻击者$\mathcal{A}$猜到哈希值G_i, M_i, W_i, Z_i, 协议终止执行, 因此有:

$$\left|Pr[\chi_3] - Pr[\chi_2]\right| \leqslant q_s/2^{l_1} \tag{6}$$

Φ_4: 如果攻击者$\mathcal{A}$猜到用户的认证秘密值A_i, 协议终止执行, 因此有:

$$\left|Pr[\chi_4] - Pr[\chi_3]\right| \leqslant q_s/2^{l_1} \tag{7}$$

Φ_5: 如果攻击者$\mathcal{A}$进行 Corrupt(U_i^a, ϕ)查询, 并计算得到C_i, 协议终止执行.

若 Corrupt$(U_i^a, z = 1,3)$, 攻击者$\mathcal{A}$猜测用户智能卡关键参数R_i, 其概率为$q_s/2^{l_1}$.

若 Corrupt$(U_i^a, \phi = 2,3)$, 攻击者$\mathcal{A}$猜测用户口令, 其概率为$C' q_s^{s'}$.

若 Corrupt$(U_i^a, \phi = 1,2)$, 攻击者$\mathcal{A}$猜测用户的生物特征, 其概率为$q_s/2^{l_2}$.

因此得到:

$$\left|Pr[\chi_5] - Pr[\chi_4]\right| \leqslant q_s/2^{l_2} + C' q_s^{s'} + q_s/2^{l_1} \tag{8}$$

Φ_6: 在该游戏中, 使用私有哈希预言机H_1'(而不是哈希预言机H_1)来计算会话密钥. 私有哈希预言机H_1'对攻击者$\mathcal{A}$来说是一无所知的, 因此, 我们有:

$$Pr[\chi_6] = \frac{1}{2} \tag{9}$$

用事件Γ_1表示攻击者$\mathcal{A}$进行哈希查询$h_1(h_1(A_i \| C_i) \| h_1(r_1 r_2 r_3 P))$. 若事件$\Gamma_1$不发生, 那么游戏$\Phi_6$与游戏$\Phi_5$是不可区分的. 因此有:

$$\left|Pr[\chi_6] - Pr[\chi_5]\right| \leqslant Pr[\Gamma_1] \tag{10}$$

如果攻击者进行过哈希查询$h_1(h_1(A_i \| C_i) \| h_1(r_1 r_2 r_3 P))$, 那么列表$\Lambda_H$必然包含$r_1 r_2 r_3 P$相关的一条记录, 也就是说, 在$\Lambda_H$中随机选择一项, 得到 ECDHP 解的概率为$\frac{1}{q_h}$, 因此有:

$$Pr[\Gamma_1] \leqslant q_h Adv_P^{\mathrm{ECDHP}} \tag{11}$$

根据公式 (1)–公式 (11), 我们有:

$$Adv_P^{ake}(\mathcal{A}) \leqslant 2C' * q_s^{s'} + \frac{(q_s+q_e)^2}{p} + \frac{6q_s + q_h^2}{2^{l_1}} + \frac{2q_s + q_f^2}{2^{l_2}} + \frac{q_\varepsilon^2}{2^{l_3}} + 2q_h Adv_P^{\mathrm{ECDHP}} \tag{12}$$

8.3 启发式安全分析

为避免 Hajian 等人[27]方案与 Wu 等人[28]方案的安全缺陷, 所提方案采用模糊验证技术、Diffie-Hellman 密钥交换、避免使用验证表等安全措施. 本节证明所提方案能够抵抗常见的安全攻击, 例如口令猜测攻击、设备捕获攻击、内部攻击、仿冒攻击, 实现前向安全性、匿名性等安全属性.

(1) 离线口令猜测攻击

所提方案引入生物特征、模糊验证+Honeywords 技术[32], 以增强用户身份认证的安全性, 保护用户口令不被破解. 为加强用户身份认证的安全性, 引入新的认证因素, 即生物特征. 生物特征是用户与生俱来的, 具有无需记忆与携带的优点, 随着手机等智能终端的普及, 生物特征认证成为一种流行的认证方式.引入生物特征认证后, 攻击者只有首先攻破用户生物特征, 才能猜测用户口令.

所提方案使用模糊验证值 V_i^*, 假设用户身份标识和口令同为 32 位, 当 $n=2^8$ 时, 将有 $\frac{2^{32}\times 2^{32}}{2^8}$ 标识口令对满足 $V_i^*=V_i$. 即使攻击者同时攻破用户智能卡与生物特征, 也无法成功猜测用户口令. 从候选口令中找出用户正确的口令, 攻击者只能通过在线猜测的方式, 逐一尝试候选口令. 所提方案采用 Honeywords 技术, 利用智能卡参数 x_i 检测口令在线猜测攻击. 攻击者获得用户智能卡后, 能够得到参数 x_i, 但此时 A_i 仍是未知的. 若 *CSP* 收到消息 $\{B_i,F_i,G_i,T_1\}$ 时, 发现 $x_i^*=x_i$, $G_i^*\neq G_i$, *CSP* 认为该消息很可能来自攻破用户智能卡的攻击者. *CSP* 从数据库中找到 $\{ID_i,\ t_i,\ Cou\}$, 执行 $Cou=Cou+1$. 当 $Cou\geqslant 10$ 时, 挂起用户智能卡, 从而有效地阻止在线猜测攻击.

同时, 基于上述技术, 所提方案实现三因素安全性, 攻击者在获取用户的任意两种认证因素的情况下, 无法揭露认证秘密值 A_i 以及用户的第 3 种认证因素.

(2) 设备捕获攻击

雾节点通常是网关、路由器、访问点这样的计算能力与存储能力受限的设备, 存在被攻破的可能. 攻击者在攻破雾节点获得其密钥后, 尝试破坏其他通信方的安全性.在所提方案中, 即使攻击者成功攻破雾节点并获得密钥 k_j, 但由于随机数 r_2 是未知的, 攻击者无法计算 $r_2\cdot r_3B_i$, 攻击者无法计算会话密钥 sk. 此外, 由于哈希函数的计算是不可逆的, 攻击者无法利用 k_j 揭示云服务器的密钥.同时, 借助密钥 k_j, 对攻破用户的认证因素、认证秘密值并无帮助. 攻击者也无法借助密钥 k_j 攻破其他雾节点的密钥. 攻击者捕获雾节点, 对用户、云服务器、其他雾节点的安全性并不产生影响. 因此, 所提方案能够抵抗设备捕获攻击. 同样的, 在攻击者与雾节点合谋的情形下, 由于秘密参数 A_i,s,k_j 对攻击者来说是不可得的, 攻击者不能冒充用户、云服务器或其他雾节点. 由于椭圆曲线 Diffie-Hellman 问题的难解性, 攻击者无法揭露会话密钥.

(3) 双向认证

在所提方案中, 用户与云服务器共享认证秘密值 A_i, 雾节点与云服务器共享密钥 k_j. 在认证与密钥协商阶段, 云服务器与雾节点根据 k_j 互相认证, 云服务器与用户根据 A_i 互相认证. 雾节点收到消息 $\{Q_i,W_i,Y_i,Z_i\}$, 若 $W_i^*=W_i$, 表明云服务器成功认证用户, 从而雾节点相信用户的真实性. 用户收到消息 $\{Q_i,W_i,Y_i,Z_i\}$, 若 $Z_i^*=Z_i$, 表明云服务器成功认证雾节点, 从而用户相信雾节点的真实性. 值得注意的一点, 用户与雾节点的双向认证是通过可信第三方 *CSP* 间接完成的, 因此在所提方案中, 当用户位置发生变化, 可直接通过新的雾节点访问 *CSP*, 不需附加额外的操作, 所提方案对于用户位置变化来说是透明的.

(4) 三方会话密钥协商

在基于雾计算的智能医疗场景中, 数据在用户、雾节点、云服务器三方之间交互, 因此认证方案要实现三方会话密钥协商. 在所提方案中, 基于椭圆曲线 Diffie-Hellman 密钥交换思想, 构建会话密钥 $sk=h_1(h_1(A_i\|C_i)\|r_1r_2r_3P)$, 只有生成随机数 r_1,r_2,r_3 的用户、雾节点、云服务器能够计算 $r_1r_2r_3P$, 会话密钥的安全性基于椭圆曲线离散对数难题. 此外, 为进一步保证安全性, 会话密钥的生成基于一个长期秘密值 $h_1(A_i\|C_i)$, 使得在某一通信方随机数泄漏的情况下, 依然无法揭露会话密钥, 保证所提方案能够抵抗临时秘密值泄漏攻击.

(5) 匿名性

所提方案实现用户匿名性以及雾节点身份标识匿名性.实现方式是基于用户 (雾节点) 选取的随机数和云服务

器公钥, 生成对称加密密钥, 加密用户身份标识和雾节点身份标识. 本质上是基于椭圆曲线 Diffie-Hellman 密钥交换, 生成对称加密密钥, 保证只有云服务器才能够解密消息, 恢复用户和雾节点身份标识. 基于选取的随机数生成用户和雾节点动态身份标识, 保证每次生成的动态身份标识都是不同的, 实现了不可追踪性.

(6) 前向安全性

所提方案基于椭圆曲线 Diffie-Hellman 密钥交换思想构建会话密钥, 只有生成随机数 r_1, r_2, r_3 的用户、雾节点、云服务器能够计算 $r_1r_2r_3P$. 即使攻击者获得云服务器密钥 s, 由于椭圆曲线离散对数难题是不可解的, 攻击者无法计算 $r_1r_2r_3P$, 所提方案实现了前向安全性.

(7) 内部攻击

在注册阶段, 用户未将口令的相关信息泄露给云服务器, 云服务器不能根据用户发送的注册请求消息, 猜测用户口令. 此外, 对用户来说, 密钥 k_j 是未知的, 用户不能够伪装成雾节点或云服务器. 同样的, 对雾节点来说, 认证秘密值 A_i 是未知的, 雾节点不能够伪装成用户或云服务器. 所提方案能够抵抗内部攻击.

(8) 仿冒攻击

在消息 $\{B_i, F_i, G_i, T_1\}$ 中, 使用认证秘密值 A_i 认证消息的真实性. 要伪造这个消息, 攻击者需要先得到 A_i. 要获得 A_i, 攻击者必须获取用户的全部 3 种认证因素. 在消息 $\{L_i, O_i, M_i, T_2\}$ 中, 使用密钥 k_j 认证消息的真实性. 要伪造这个消息, 攻击者需要先得到 k_j. 在消息 $\{Q_i, W_i\}$ 中, 云服务器使用密钥 k_j 认证消息的真实性, 在消息 $\{Y_i, Z_i\}$ 中, 使用认证秘密值 A_i 认证消息的真实性. 攻击者无法获得 A_i 和 k_j, 所提方案能够抵抗仿冒攻击.

(9) 良好可修复性

首先, 当用户智能卡丢失或被盗时, 通过执行用户重注册阶段, 用户向 *CSP* 重新注册, *CSP* 为用户生成新的认证参数. *CSP* 通过选取新的随机数 x_i, 得到用户新的认证秘密值 A_i, 旧的智能卡将自动撤销; 其次, 用户口令或生物特征泄漏时, 通过执行用户口令与生物特征更新阶段, 用户可在本地更新其口令与生物特征; 再次, 所提方案支持动态雾节点增加阶段, 新的雾节点可随时加入, 提供新的计算资源, 分担计算任务; 因此, 所提方案实现良好可修复性.

9 对比分析

本节将所提方案与基于智能医疗的同类方案的安全性与效率进行对比. 表 2 给出所提方案与同类方案安全属性分析的结果. 其中, 文献 [23,24,26,27] 是基于哈希函数的方案. 文献 [34−37] 为基于椭圆曲线密码系统的方案. 文献 [25,28] 是基于双线性对的方案. 文献 [25,28,36,37] 为基于雾计算的方案. 表 2 表明, 基于哈希函数的方案[23,24,26,27]存在诸多安全缺陷, 在会话密钥的安全性方面同样差强人意. 基于椭圆曲线密码系统的方案[34−37]相比基于哈希函数的方案[23,24,26,27], 具有更好的安全性, 但依然存在安全缺陷, 例如, 遭受设备捕获攻击, 未实现前向安全性. 基于双线性对的方案[25,28], 遭受临时秘密值泄漏攻击、离线口令猜测攻击. 在会话密钥安全性方面, 除所提方案之外, 只有文献 [28] 方案构建了安全的会话密钥, 能够抵抗针对会话密钥的各种已知攻击. 相比同类方案, 所提方案能够构建安全的三方会话密钥, 实现身份匿名性、三因素安全性等安全属性, 并且对于已知攻击是安全的.

文献 [24,28,36] 等方案因智能卡存储验证值, 而导致方案遭受离线口令猜测攻击. 文献 [25,26] 的方案不支持本地口令验证, 虽然能够避免离线口令猜测攻击, 但在登录消息到达服务器端时, 才能验证用户输入口令的正确性, 由此带来延迟与网络带宽浪费.由此可见, 离线口令猜测攻击是一种常见且严重影响安全性的攻击. 所提方案采用模糊验证+Honeywords 技术, 抵抗离线口令猜测攻击.

表 3 将所提方案与同类方案的计算开销与通信开销进行对比分析. 其中, T_H 表示 MD5 哈希运算, T_M 表示椭圆曲线点乘运算, T_S 表示 AES 对称加密/解密运算, T_P 表示双线性对运算. 基于开源密码库 MIRCAL, 在搭载 I5-4460S 2.90 GHz 处理器, 4 GB 内存, Windows 8 操作系统的个人电脑上实现相关密码运算, 实验结果显示, T_H、T_M、T_S、T_P 的计算时间分别为 0.007 ms、2.165 ms、0.013 ms、5.427 ms[38]. 异或运算的计算时间忽略不计. 在评估通信开销时, 假设用户和雾节点的身份标识及动态身份标识、随机数、时间戳为 128 bit, MD5 哈希值与 AES 加密输出的长度为 128 bit, 椭圆曲线群上的点为 160 bit.

表 2　与同类方案安全属性比较

安全属性	文献[24]	文献[27]	文献[23]	文献[26]	文献[35]	文献[34]	文献[25]	文献[28]	文献[36]	文献[37]	所提方案
用户匿名性	√	√	√	√	√	√	√	√	√	√	√
本地口令验证	√	√	√	×	√	√	×	√	√	√	√
抵抗离线口令猜测攻击	×	√	√	√	√	√	√	×	×	√	√
抵抗仿冒攻击	×	×	×	√	√	√	√	×	×	√	√
验证表丢失攻击	√	×	√	√	√	√	√	√	√	√	√
抵抗内部攻击	×	√	√	×	√	√	√	√	√	√	√
抵抗拒绝服务攻击	√	×	×	×	√	√	√	√	√	√	√
重放攻击	√	√	×	√	×	√	√	√	√	√	√
设备捕获攻击	×	×	×	×	√	×	√	√	√	×	√
抵抗会话密钥泄露攻击	√	√	×	√	√	√	√	√	√	√	√
抵抗临时秘密值泄露攻击	×	√	×	√	×	√	×	√	×	√	√
前向安全性	×	×	×	×	√	×	√	√	√	×	√
会话密钥安全性	×	×	×	×	×	×	×	√	×	×	√
三因素安全性	—	—	×	—	√	×	—	—	—	×	√

注: “√”表示方案能够抵抗该攻击, “×”表示方案未能抵抗该攻击, “—”表示方案不支持评估该项安全属性

表 3　与同类方案计算与通信开销比较

方案	计算开销			通信开销 (bits)		
	用户	*CSP*/网关	雾节点/传感设备	用户	*CSP*/网关	雾节点/传感设备
Gupta等人[24]	$4T_H$	$7T_H$	$5T_H$	1 664	512	512
Hajian等人[27]	$12T_H$	$7T_H$	$9T_H$	1 792	512	512
Amin等人[23]	$14T_H$	$17T_H$	$4T_H$	768	896	256
Fotouhi等人[26]	$10T_H$	$14T_H$	$6T_H$	640	1 408	384
Li等人[35]	$10T_H+3T_M$	$8T_H$	$4T_H+2T_M$	544	832	416
Soni等人[34]	$13T_H+3T_M$	$12T_H+3T_M$	$5T_H$	672	1 184	384
Jia等人[25]	$5T_H+2T_M+1T_P$	$4T_H+2T_M+1T_P$	$9T_H+3T_M+1T_P$	544	544	1 664
Wu等人[28]	$14T_H+2T_M+1T_P$	$10T_H+3T_M+1T_P$	$4T_H+2T_M+1T_P$	544	544	1 664
Ma等人[36]	$4T_H+3T_M$	$11T_H+10T_M$	$4T_H+4T_M$	1 280	1 248	864
Wazid等人[37]	$18T_H+2T_M$	$12T_H+3T_M$	$13T_H$	800	800	672
所提方案	$6T_H+3T_M+2T_S$	$10T_H+4T_M+4T_S$	$4T_H+3T_M+2T_S$	544	544	1 376

同类方案中, 基于哈希函数的方案虽然效率较高, 但智能医疗中的数据具有高度敏感性, 要求认证方案具有高安全性, 基于哈希函数的方案不能满足智能医疗场景的高安全性要求. 基于双线性对的方案涉及较高的计算开销. 基于椭圆曲线密码系统的方案, 相比基于哈希函数的方案实现更好的安全性, 但依然遭受设备捕获攻击、前向安全性等安全缺陷.

相比雾架构的同类方案, 所提方案在安全性方面有明显提高, 且有良好的效率. 图 2 将所提方案的计算与通信开销与基于雾计算的同类方案相比较. 结果表明, 所提方案的总计算开销与总通信开销处于第 2 位, 略高于 Wazid 等人[37]方案, 这是因为所提方案使用额外的计算量, 弥补 Wazid 等人[37]方案的安全缺陷, 使得方案能够抵抗设备捕获攻击, 实现前向安全性.

10　结束语

借助雾计算技术, 能很好地解决, 数据上传到远程云服务器所带来的额外通信开销与传输时延问题. 本文对两

个智能医疗认证协议进行安全分析, 指出 Hajian 等人协议无法抵抗验证表丢失攻击、拒绝服务攻击、设备捕获攻击、会话密钥泄漏攻击, 指出 Wu 等人协议无法抵抗离线口令猜测攻击与仿冒攻击. 提出一个基于雾计算的智能医疗三方认证与密钥协商协议, 所提方案相比同类方案, 具有更好的安全性和效率, 能更好的为基于雾计算的智能医疗场景的数据访问与传输提供安全保护. 由于区块链具有去中心化、不需要可信第三方的优点, 基于当前的研究工作, 下一步我们计划研究雾计算环境下基于区块链的物联网用户认证协议.

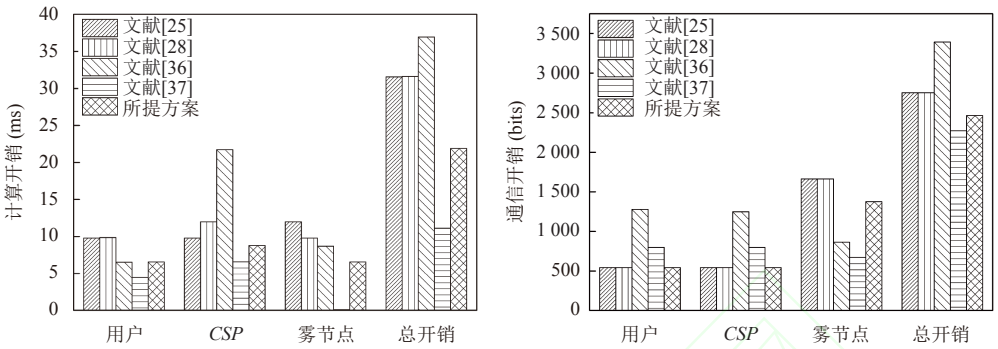

图 2 与雾架构同类方案计算与通信开销比较

References:

[1] Wang CY, Wang D, Tu Y, Xu GA, Wang HX. Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Trans. on Dependable and Secure Computing, 2022, 19(1): 507–523. [doi: 10.1109/TDSC.2020.2974220]

[2] Wang D, Li WT, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. on Industrial Informatics, 2018, 14(9): 4081–4092. [doi: 10.1109/TII.2018.2834351]

[3] Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang MZ, Liljeberg P. Exploiting smart e-Health gateways at the edge of healthcare internet-of-things: A fog computing approach. Future Generation Computer Systems, 2018, 78: 641–658. [doi: 10.1016/j.future.2017.02.014]

[4] Li WT, Wang D, Wang P. Insider attacks against multi-factor authentication protocols for wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2019, 30(8): 2375−2391 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5766.htm [doi: 10.13328/j.cnki.jos.005766]

[5] Wang CY, Wang D, Wang FF, Xu AG. Multi-factor user authentication scheme for multi-gateway wireless sensor networks. Chinese Journal of Computers, 2020, 43(4): 683–700 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2020.00683]

[6] Hu XX, Zhang QH, Zhang ZF, Liu FM. Universally composable gateway-oriented password-authenticated key exchange protocol. Chinese Journal of Computers, 2017, 40(5): 1109–1120 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2017.01109]

[7] Das AK, Wazid M, Kumar N, Vasilakos AV, Rodrigues JJPC. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment. IEEE Internet of Things Journal, 2018, 5(6): 4900–4913. [doi: 10.1109/JIOT.2018.2877690]

[8] Wang D, Li WT, Wang P. Crytanalysis of three anonymous authentication schemes for multi-server environment. Ruan Jian Xue Bao/Journal of Software, 2018, 29(7): 1937−1952 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[9] Wei FS, Ma JF, Li GS, Ma CG. Efficient three-party password-based authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016, 27(9): 2389−2399 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4861.htm [doi: 10.13328/j.cnki.jos.004861]

[10] He DB, Zeadally S, Kumar N, Wu W. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE Trans. on Information Forensics and Security, 2016, 11(9): 2052–2064. [doi: 10.1109/TIFS.2016.2573746]

[11] Alrawais A, Alhothaily A, Hu CQ, Cheng XZ. Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet

Computing, 2017, 21(2): 34–42. [doi: 10.1109/MIC.2017.37]

[12] Wu ZY, Lee YC, Lai FP, Lee HC, Chung Y. A secure authentication scheme for telecare medicine information systems. Journal of Medical Systems, 2012, 36(3): 1529–1535. [doi: 10.1007/s10916-010-9614-9]

[13] Huang XY, Chen XF, Li J, Xiang Y, Xu L. Further observations on smart-card-based password-authenticated key agreement in distributed systems. IEEE Trans. on Parallel and Distributed Systems, 2014, 25(7): 1767–1775. [doi: 10.1109/TPDS.2013.230]

[14] He DB, Kumar N, Chen JH, Lee CC, Chilamkurti N, Yeo SS. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 2015, 21(1): 49–60. [doi: 10.1007/s00530-013-0346-9]

[15] Li X, Niu JW, Kumari S, Liao JG, Liang W, Khan MK. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Security and Communication Networks, 2016, 9(15): 2643–2655. [doi: 10.1002/sec.1214]

[16] Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KKR. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks, 2017, 129: 429–443. [doi: 10.1016/j.comnet.2017.03.013]

[17] Koya AM, Deepthi PP. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. Computer Networks, 2018, 140: 138–151. [doi: 10.1016/j.comnet.2018.05.006]

[18] Wu F, Li X, Xu LL, Kumari S, Karuppiah M, Shen J. A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. Computers & Electrical Engineering, 2017, 63: 168–181. [doi: 10.1016/j.compeleceng.2017.04.012]

[19] Das AK, Wazid M, Kumar N, Khan MK, Choo KKR, Park Y. Design of secure and lightweight authentication protocol for wearable devices environment. IEEE Journal of Biomedical and Health Informatics, 2018, 22(4): 1310–1322. [doi: 10.1109/JBHI.2017.2753464]

[20] Wu F, Li X, Sangaiah AK, Xu LL, Kumari S, Wu LX, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems, 2018, 82: 727–737. [doi: 10.1016/j.future.2017.08.042]

[21] Wazid M, Das AK, Vasilakos AV. Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications, 2018, 123: 112–126. [doi: 10.1016/j.jnca.2018.09.008]

[22] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Proc. of the 2004 Int'l Conf. on the Theory and Applications of Cryptographic Techniques . Interlaken: Springer, 2004. 523−540. [doi: 10.1007/978-3-540-24676-3_31]

[23] Amin R, Islam SKH, Biswas GP, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems, 2018, 80: 483–495. [doi: 10.1016/j.future.2016.05.032]

[24] Gupta A, Tripathi M, Shaikh TJ, Sharma A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. Computer Networks, 2019, 149: 29–42. [doi: 10.1016/j.comnet.2018.11.021]

[25] Jia XY, He DB, Kumar N, Choo KKR. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks, 2019, 25(8): 4737–4750. [doi: 10.1007/s11276-018-1759-3]

[26] Fotouhi M, Bayat M, Das AK, Far HAN, Pournaghi SM, Doostari MA. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks, 2020, 177: 107333. [doi: 10.1016/j.comnet.2020.107333]

[27] Hajian R, ZakeriKia S, Erfani SH, Mirabi M. SHAPARAK: Scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement. Computer Networks, 2020, 183: 107567. [doi: 10.1016/j.comnet.2020.107567]

[28] Wu TY, Wang T, Lee YQ, Zheng WM, Kumari S, Kumar S. Improved authenticated key agreement scheme for fog-driven IoT healthcare system. Security and Communication Networks, 2021, 2021: 6658041. [doi: 10.1155/2021/6658041]

[29] Wang D, He DB, Wang P, Chu CH. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. on Dependable and Secure Computing, 2015, 12(4): 428–442. [doi: 10.1109/TDSC.2014.2355850]

[30] Feng DG, Xu J, Lan X. Study on 5G mobile communication network security. Ruan Jian Xue Bao/Journal of Software, 2018, 29(6): 1813–1825 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5547.htm [doi: 10.13328/j.cnki.jos.005547]

[31] Yang L, Ma JF, Jiang Q. Direct anonymous attestation scheme in cross trusted domain for wireless mobile networks. Ruan Jian Xue Bao/Journal of Software, 2012, 23(5): 1260−1271 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4052.htm [doi: 10.3724/SP.J.1001.2012.04052]

[32] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2018, 15(4): 708–722. [doi: 10.1109/TDSC.2016.2605087]

[33] Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks. In: Proc. of the 2000 Int'l Conf. on the Theory and Application of Cryptographic Techniques. Bruges: Springer, 2000. 139–155. [doi: 10.1007/3-540-45539-6_11]

[34] Soni P, Pal AK, Islam SKH. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput. Computer Methods and Programs in Biomedicine, 2019, 182: 105054. [doi: 10.1016/j.cmpb.2019.105054]

[35] Li X, Peng JY, Obaidat MS, Wu F, Khan MK, Chen CY. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal, 2020, 14(1): 39–50. [doi: 10.1109/JSYST.2019.2899580]

[36] Ma MM, He DB, Wang HQ, Kumar H, Choo KKR. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. IEEE Internet of Things Journal, 2019, 6(5): 8065–8075. [doi: 10.1109/JIOT.2019.2902840]

[37] Wazid M, Das AK, Kumar N, Vasilakos AV. Design of secure key management and user authentication scheme for fog computing services. Future Generation Computer Systems, 2019, 91: 475–492. [doi: 10.1016/j.future.2018.09.017]

[38] He DB, Kumar N, Khan MK, Wang LN, Shen J. Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Systems Journal, 2018, 12(2): 1621–1631. [doi: 10.1109/JSYST.2016.2633809]

[39] Burrows M, Abadi M, Needham RM. A logic of authentication. Proc. of the Royal Society A: Mathematical, Physical and Engineering Sciences, 1989, 426(1871): 233–271. [doi: 10.1098/rspa.1989.0125]

附中文参考文献:

[4] 李文婷, 汪定, 王平. 无线传感器网络下多因素身份认证协议的内部人员攻击. 软件学报, 2019, 3(8): 2375−2391. http://www.jos.org.cn/1000-9825/5766.htm [doi: 10.13328/j.cnki.jos.005766]

[5] 王晨宇, 汪定, 王菲菲, 徐国爱. 面向多网关的无线传感器网络多因素认证协议. 计算机学报, 2020, 43(4): 683–700. [doi: 10.11897/SP.J.1016.2020.00683]

[6] 胡学先, 张启慧, 张振峰, 刘凤梅. 通用可组合的网关口令认证密钥交换协议. 计算机学报, 2017, 40(5): 1109–1120. [doi: 10.11897/SP.J.1016.2017.01109]

[8] 汪定, 李文婷, 王平. 对三个多服务器环境下匿名认证协议的分析. 软件学报, 2018, 29(7): 1937−1952. http://www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[9] 魏福山, 马建峰, 李光松, 马传贵. 标准模型下高效的三方口令认证密钥交换协议. 软件学报, 2016, 27(9): 2389−2399. http://www.jos.org.cn/1000-9825/4861.htm [doi: 10.13328/j.cnki.jos.004861]

[30] 冯登国, 徐静, 兰晓. 5G移动通信网络安全研究. 软件学报, 2018, 29(6): 1813−1825. http://www.jos.org.cn/1000-9825/5547.htm [doi: 10.13328/j.cnki.jos.005547]

[31] 杨力, 马建峰, 姜奇. 无线移动网络跨可信域的直接匿名证明方案. 软件学报, 2012, 23(5): 1260−1271. http://www.jos.org.cn/1000-9825/4052.htm [doi: 10.3724/SP.J.1001.2012.04052]

附录 A

BAN 逻辑证明[39]是一种基于逻辑的安全证明方法, 用于验证安全协议是否实现特定功能. 我们运用 BAN 逻辑证明所提方案实现三方相互认证与会话密钥协商. BAN 逻辑使用的符号和规则如表 A.1 所示.

下面给出所提方案应实现安全目标的形式化表示 (G1–G6), 表示所提方案在用户、雾节点、云服务器之间实现三方相互认证与会话密钥协商.

G1: $U_i| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

G2: $U_i| \equiv S| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

G3: $F_j| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

G4: $F_j| \equiv S| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

G5: $S| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

G6: $S| \equiv F_j| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$

所提方案的证明基于以下形式化假设 (A1–A15).

A1: $S| \equiv S \overset{A_i}{\longleftrightarrow} U_i$

A2: $S| \equiv \#(r_1 P)$

A3: $S| \equiv U_i \Rightarrow U_i \overset{C_i}{\longleftrightarrow} S$

A4: $S| \equiv S \overset{k_j}{\longleftrightarrow} F_j$

表 A.1 BAN 逻辑中的符号

符号	描述
P,Q	主体
X,Y	公式
K	密钥
$\#(X)$	X是新鲜的
$P\mid\sim X$	P曾经发送X
$P\triangleleft X$	P收到X
$P\mid\equiv X$	P相信X的真实性
$P\Rightarrow X$	P对X具有管辖权
$P\overset{K}{\leftrightarrow}Q$	K为P与Q共享的密钥
$\{X\}_K$	用密钥K加密X
$P\overset{Y}{\longleftrightarrow}Q$	Y为P与Q共享的秘密
$\langle X\rangle_Y$	X与秘密Y合成得到的消息
临时值验证规则	$\dfrac{P\mid\equiv\#(X),Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$, 如果$P$相信$X$的新鲜性, P相信Q发送了X, 那么P相信Q相信X
管辖规则	$\dfrac{P\mid\equiv Q\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$, 如果$P$相信$Q$对$X$具有管辖权, P相信Q相信X, 那么P相信X为真
	第1种情形$\dfrac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,P\triangleleft\{X\}_K}{P\mid\equiv Q\mid\sim X}$, P相信K是它与Q共享的密钥, P收到密钥K. 加密X得到的消息, 那么P相信Q发送了X
消息含义规则	第2种情形$\dfrac{P\mid\equiv P\overset{Y}{\longleftrightarrow}Q,P\triangleleft\langle X\rangle_Y}{P\mid\equiv Q\mid\sim X}$, P. 相信Y是它与Q共享的秘密, P收到X与秘密Y合成得到的消息, 那么P相信Q发送了X

A5: $S\mid\equiv\#(r_2P)$

A6: $S\mid\equiv F_j\Rightarrow\left\langle F_j\overset{N_i}{\longleftrightarrow}S,\{r_2B_i\}_{N_i}\right\rangle$

A7: $S\mid\equiv F_j\Rightarrow\left(S\overset{SK}{\longleftrightarrow}U_i\overset{SK}{\longleftrightarrow}F_j\right)$

A8: $F_j\mid\equiv S\overset{k_j}{\longleftrightarrow}F_j$

A9: $F_j\mid\equiv\#(r_3B_i)$

A10: $F_j\mid\equiv S\Rightarrow\langle r_3B_i,h_1(A_i\parallel C_i)\rangle$

A11: $F_j\mid\equiv S\Rightarrow S\overset{SK}{\longleftrightarrow}U_i\overset{SK}{\longleftrightarrow}F_j$

A12: $U_i\mid\equiv S\overset{A_i}{\longleftrightarrow}U_i\ \ U_i\mid\equiv S\overset{C_i}{\longleftrightarrow}U_i$

A13: $U_i\mid\equiv\#(r_3N_i)$

A14: $U_i\mid\equiv S\mid\Rightarrow r_3N_i$

A15: $U_i\mid\equiv S\Rightarrow\left(S\overset{SK}{\longleftrightarrow}U_i\overset{SK}{\longleftrightarrow}F_j\right)$

下面给出所提方案消息的理想化形式.

M1: $U_i\rightarrow S\left\langle r_1P,U_i\overset{C_i}{\longleftrightarrow}S\right\rangle_{A_i}$

M2: $F_j\rightarrow S\left\langle r_2P,F_j\overset{N_i}{\longleftrightarrow}S,\{r_2B_i\}_{N_i}\right\rangle_{k_j}$

M3: $S\rightarrow F_j\{r_3B_i,h_1(A_i\parallel C_i)\}_{k_j}$

M4: $S_j \rightarrow U_i : <\{r_3 N_i\}_{C_i}>_{A_i}$

所提方案的证明过程如下:

由消息 M1, 得到 S1: $S \triangleleft \left\langle r_1 P, U_i \overset{C_i}{\longleftrightarrow} S \right\rangle_{A_i}$

由 S1 与 A1, 运用消息含义规则, 得到 S2: $S| \equiv U_i| \sim \left\langle r_1 P, U_i \overset{C_i}{\longleftrightarrow} S \right\rangle$

由 S2 与 A2, 运用临时值验证规则, 得到 S3: $S| \equiv U_i| \equiv \left\langle r_1 P, U_i \overset{C_i}{\longleftrightarrow} S \right\rangle$

由 S3 与 A3, 运用管辖规则, 得到 S4: $S| \equiv U_i \overset{C_i}{\longleftrightarrow} S$

从消息 M2, 得到 S5: $S \triangleleft \left\langle r_2 P, F_j \overset{N_i}{\longleftrightarrow} S, \{r_2 B_i\}_{N_i} \right\rangle_{k_j}$

由 S5 与 A4, 运用消息含义规则, 得到 S6: $S| \equiv F_j| \sim \left\langle r_2 P, F_j \overset{N_i}{\longleftrightarrow} S, \{r_2 B_i\}_{N_i} \right\rangle$

由 S6 与 A5, 运用临时值验证规则, 得到 S7: $S| \equiv F_j| \equiv \left\langle r_2 P, F_j \overset{N_i}{\longleftrightarrow} S, \{r_2 B_i\}_{N_i} \right\rangle$

由 S7 与 A6, 运用管辖规则, 得到 S8: $S| \equiv F_j \overset{N_i}{\longleftrightarrow} S$ 与 S9: $S| \equiv \{r_2 B_i\}_{N_i}$

由 S8 与 S9, 得到 S10: $S| \equiv r_2 B_i$

由 S10 与 $sk = h_1(h_1(A_i \| C_i) \| r_3 \cdot r_2 B_i))$, 得到 S11: $S| \equiv F_j| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$ (G6)

由 S11 与 A7, 运用管辖规则, 得到 S12: $S| \equiv S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j$ (G5)

从消息 M3, 得到 S13: $F_j \triangleleft \{r_3 B_i, h_1(A_i \| C_i)\}_{k_j}$

由 S13 与 A8, 运用消息含义规则, 得到 S14: $F_j| \equiv S| \sim \langle r_3 B_i, h_1(A_i \| C_i)\rangle$

由 S14 与 A9, 运用临时值验证规则, 得到 S15: $F_j| \equiv S| \equiv \langle r_3 B_i, h_1(A_i \| C_i)\rangle$

由 S15 与 A10, 运用管辖规则, 得到 S16: $F_j| \equiv \langle r_3 B_i, h_1(A_i \| C_i)\rangle$

由 S16 及 $sk = h_1(h_1(A_i \| C_i) \| r_2 \cdot r_3 B_i))$, 得到 S17: $F_j| \equiv S| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$ (G4)

由 S17 及 A11, 运用管辖规则, 得到 S18: $F_j| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$ (G3)

从消息 M4, 得到 S19: $U_i \triangleleft <\{r_3 N_i\}_{C_i}>_{A_i}$

由 S19 及 A12, 运用消息含义规则, 得到 S20: $U_i| \equiv S| \sim r_3 N_i$

由 S20 及 A13, 运用临时值验证规则, 得到 S21: $U_i| \equiv S| \equiv r_3 N_i$

由 S21 及 A14, 运用管辖规则, 得到 S22: $U_i| \equiv r_3 N_i$

由 S22 及 $sk = h_1(h_1(A_i \| C_i) \| r_1 \cdot r_3 N_i))$, 得到 S23: $U_i| \equiv S| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$ (G2)

由 S23 及 A15, 运用管辖规则, 得到 S24: $U_i| \equiv \left(S \overset{SK}{\longleftrightarrow} U_i \overset{SK}{\longleftrightarrow} F_j\right)$ (G1)

王菲菲(1991－), 女, 博士, 讲师, CCF 专业会员, 主要研究领域为物联网安全, 多因子认证协议.

汪定(1985－), 男, 教授, 博士生导师, CCF 高级会员, 主要研究领域为数字身份安全.