面向无线传感器网络的多因素安全增强认证协议

张凌浩[1,2]，梁晖辉[1,2]，邓 东[3]，刘洋洋[3]，唐 超[1,2]，常政威[1,2]，桂盛霖[3*]

(1. 国网四川省电力公司电力科学研究院 成都 610072；2. 电力物联网四川省重点实验室 成都 610031；
3. 电子科技大学计算机科学与工程学院 成都 611731)

【摘要】为解决现有协议普遍存在的离线字典攻击、缺少匿名性、无前向安全等安全缺陷，基于最新安全模型，将KSSTI 攻击和注册合法用户攻击加入安全模型评价标准中，形成增强安全模型，提出了一种面向无线传感器网络的多因素安全增强认证协议，实现了用户通过网关与传感器节点两端的安全会话密钥协商。BAN 逻辑和启发式分析结果表明该协议实现了双向认证，满足匿名性、前向安全、抵抗内部攻击、抵抗 KSSTI 攻击等重要安全属性。相比于已有协议，该文协议的安全等级更高且计算量与通信量适中，适用于安全等级要求高且传感器节点计算资源受限的应用场景。

关 键 词 认证协议； 增强安全模型； 三因素； 无线传感器网络
中图分类号 TP309.08 **文献标志码** A doi:10.12178/1001-0548.2022238

Multi-Factor Security Enhanced Authentication Protocol for Wireless Sensor Networks

ZHANG Linghao[1,2], LIANG Huihui[1,2], DENG Dong[3], LIU Yangyang[3], TANG Chao[1,2], CHANG Zhengwei[1,2], and GUI Shenglin[3*]

(1. State Grid Sichuan Eletric Power Research Institute Chengdu 610072;
2. Power Internet of Things Key Laboratory of Sichuan Province Chengdu 610031;
3. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract To solve security defects generally lain in many existing protocols, such as offline dictionary attack, lack of anonymity and no forward security, based on the latest security model, this paper adds KSSTI attack and registered legitimate user attack into the security model evaluation standard to form an enhanced security model. Based on this enhanced security model, a multi-factor security enhanced authentication protocol for wireless sensor networks is proposed, which realizes the secure session key negotiation among users and sensor nodes through the gateway. The results of BAN logic and heuristic analysis show that the protocol realizes two-way authentication and meets the important security attributes of anonymity, forward security, resistance to internal attacks, resistance to KSSTI attacks and so on. Compared with the existing protocols, this protocol has higher security level and moderate amount of computation and communication. It is suitable for the application scenarios with high security level requirements and limited computing resources of sensor nodes.

Key words authentication protocol; enhanced security model; three-factor; wireless sensor networks

随着人们对智能生活的追求，物联网在医疗[1]、家居[2]、农业[3]、战场监视[4]等领域得到广泛应用。作为物联网的重要组成部分，无线传感器网络引起了工业界和学术界越来越多的关注[5]。无线传感器网络 (wireless sensor network, WSN) 由大量的传感器节点互联组成，常部署在无人看管或恶劣环境中用于执行各类感知环境的任务，由此使得无线传感器网络容易遭受各种攻击。因此，在高安全需求的 WSN 场景下，如医疗及战场监视，面对更加强大的敌手攻击能力，要求协议能具备更多的安全属性。如何针对强大的敌手能力以及传感器节点计算和存储资源受限问题，设计出一个适用于高安全

收稿日期：2022－07－15；修回日期：2023－03－28
基金项目：国家自然科学基金 (61401067)；四川省科技重大专项 (2018GZDZX0009)；四川省重点研发项目 (2023YFG0112)
作者简介：张凌浩 (1985－)，男，博士，高级工程师，主要从事电力信息安全技术方面的研究.
*通信作者：桂盛霖，E-mail：shenglin_gui@uestc.edu.cn

场景下的面向网关的身份认证协议亟需解决。

一个典型的面向网关的无线传感器网络模型[6]包括三类参与方：传感器节点、网关和用户。传感器节点通过其所属的网关节点 (GWN) 连接到互联网，用户通过访问 GWN 读取其管理的传感器节点的数据。该模型下，用户、GWN 以及节点间均通过公共信道发送消息，并且攻击者可监听或者更改公共信道上传递的消息。按照认证用户身份所使用的因素个数可分为单因素[7]、双因素[8] 和三因素[9]，通常含有两个及以上的认证因素被称为多因素协议。单因素协议仅仅使用用户密码作为用户身份认证，由于用户密码信息具有低熵性，使得用户密码容易被猜测破解[10]。双因素协议在前者基础上增加了智能卡作为用户身份认证的第二个要素。随后考虑到用户智能卡易丢失，三因素协议继续引入了用户生物特性作为用户身份认证的第三个要素。由于每个用户的生物特征是独一无二的，相比双因素协议更能保证网络安全，因此三因素协议常常被应用在高安全场景下。

目前双因素和三因素协议所考虑的安全模型存在一定差异，主要体现在敌手能力的强弱以及评价标准是否全面。因此在不同的安全模型下，已有文献所提出的协议安全性存在较大差异。

文献 [11] 针对文献 [12] 中方案存在离线字典猜测攻击、前向安全等问题提出自己的双因素协议并用 BAN 逻辑证明了其安全性，随后被文献 [13] 指出其存在内部攻击、智能卡丢失攻击、前向安全性问题。此外，文献 [13] 还指出文献 [14] 的方案与文献 [12] 存在相同的缺陷，并针对文献 [14] 和文献 [11] 存在的安全缺陷给出了解决思路。文献 [15] 将传感器节点区分为簇头和簇成员两类并提出双因素认证协议，但不能抵御 KSSTI 攻击。

随着生物技术的快速发展，为了提升身份认证的安全性，引入了生物特征，使得三因素协议得到广泛的关注。文献 [16] 提出了一种三因素认证协议，并指出了文献 [17] 的协议不能抵抗 KSSTI (known session-specific temporary information) 攻击且节点之间需要时钟同步，不适用于无线传感器网络等问题。文献 [18] 指出文献 [19] 无后向安全性、存在 KSSTI 攻击、也不适合无线传感器网络环境等缺点，但本文发现文献 [18] 所提出的改进协议仍然存在中间人攻击等安全漏洞。文献 [20] 分别针对文献 [21] 和文献 [22] 的协议存在离线字典攻击、前向安全、内部攻击等问题提出增强型方案，但其方案执行过程中所有成员共计需要 6 次公钥乘操作，计算量相比其他方案偏高。文献 [23] 指出文献 [24] 存在离线字典攻击、前向安全等问题，并提出了改进方案，然而其方案不能满足本文所考虑的更强安全模型下的安全性。

基于上述分析，可以看出已有文献若放置于后期提出的更高安全性的安全模型下会存在不足或问题。因此本文经过对已有安全模型的系统性分析和整理，选择目前最新的安全模型[6,25] 开展研究，设计满足其评价标准的三因素高效身份认证协议。如何面对更加强大的敌手能力构建高效安全的身份认证协议是保证高安全 WSN 应用场景安全性的基础问题。本文的贡献包括以下 3 个方面。

1) 通过分析文献 [16]，指出其协议无法抵抗注册合法用户攻击，从而引发传感器秘钥泄露、用户欺骗攻击、用户伪装攻击等问题；通过分析文献 [20]，指出其协议存在 KSSTI 攻击。

2) 本文基于最新的安全模型[6,25]，在其评价标准中增加抵抗 KSSTI 攻击和注册合法用户攻击，进一步增强了其评价标准，提高协议的安全等级。

3) 与文献 [15,21,22] 的三方共享会话密钥模式不同，本文的会话秘钥协商仅限于用户和传感器节点两方，在用户和传感器节点两端分别使用临时公私钥实现前向安全属性；BAN 逻辑证明和启发式分析表明，本文协议能够实现双向认证、安全的协商会话秘钥以及抵抗各类已知攻击；与相关协议相比该协议不仅可以满足增强后的安全模型的评价标准，计算量和通信量也适中，因此适用于高安全 WSN 场景下的应用。

1 安全模型及符号定义

对于一个用户身份认证协议，即使用于生成会话 SK 的临时秘密泄露，如各方用于直接计算 SK 的随机数泄露，仍能保证 SK 的安全，则称其能抵抗 KSSTI 攻击。另外，在实际场景中，攻击者极有可能注册成为合法用户与节点进行通信，由此获取系统中其他会话中的秘密信息，如文献 [15,20] 均存在此类注册合法用户攻击问题。由此可见若未考虑上述两种攻击，协议将不能保证生成会话秘钥的安全性。因此本文对文献 [6,25] 提出的安全模型做出增强，将 KSSTI 攻击和注册合法用户攻击加入其评价标准中。

1.1 攻击模型

外网用户访问网内传感器节点的场景中攻击者

具有如下能力：

C1: 攻击者能够在公开信道中任意监听、截获、注入实体间交互的信息；

C2: 攻击者知道用户 ID 空间 D_{ID} 和密码空间 D_{pw}，可以穷举该空间中的所有元素；

C3: 在 n 因素保证安全的协议中，攻击者可以获得任意 n-1 因素；

C4: 攻击者能够得到之前协商的所有对称秘钥；

C5: 在评估前向安全时攻击者能够得到所有的长期秘密；

C6: 攻击者可以攻击部分节点获取其全部的秘密；

C7: 攻击者能够注册成合法用户或合法节点同网内实体交互。

1.2　评价标准

本节给出本文所使用的评价标准，该标准包含 11 条评价指标，其中将 KSSTI 攻击加入到 S4 条，新增 S11 抗注册合法用户攻击，具体如下。

S1: 无口令验证表，要求网关和传感器节点上不应该存储用户信息相关的验证表；

S2: 口令友好性，要求用户能在本地更改用户口令；

S3: 口令安全性，用户口令不能被内部特权管理员获取或计算出来；

S4: 抗各类已知攻击，协议能够抵抗仿冒攻击、离线字典猜测攻击、重放攻击、中间人攻击、平行会话攻击、验证表丢失攻击、节点捕获攻击、网关绕过攻击、未知密钥共享攻击和已知密钥攻击、KSSTI 攻击、智能卡丢失攻击；

S5: 可修复性，要求协议支持智能卡撤销及传感器节点动态加入；

S6: 建立会话秘钥，协商完成后用户与传感器节点之间建立会话秘钥；

S7: 无时钟同步，避免因时钟同步产生的延迟影响系统的运行；

S8: 双向认证，通信的双方需要相互认证身份的合法性；

S9: 用户匿名性，要求协议能保证用户的不可追踪性；

S10: 前向安全属性，要求协议的长期秘密暴露对之前协商的会话安全性无影响；

S11: 抗注册合法用户攻击，攻击者无法通过注册合法用户来提高攻击优势。

1.3　所用符号及定义

本文用到的符号及其含义如表 1 所示。

表 1　符号描述

符号	描述	符号	描述
U_i / GWN / SN_j	用户i / 网关节点 / 传感器节点j	SK	对称秘钥
ID_i / SID_j	U_i的身份号 / SN_j的身份号	$h(\cdot)$	一种安全的哈希函数
$\mathrm{Gen}(\cdot)$	生物特征生成函数	PW_i	U_i的密码
$\mathrm{Rep}(\cdot)$	生物特征恢复函数	Bio_i	U_i的生物特征
$\|\|$ / $\oplus$	连接操作 / 异或操作	SC_i	U_i的智能卡
⟹	安全信道	→	公共信道

2　已有协议的安全性分析

2.1　文献 [16] 协议的问题分析

1) 注册合法用户攻击

A 注册完合法用户后，通过在登录认证过程中截取 $\{M_8, M_9, M_{10}, M_{11}\}$，由此可计算 $K_{\mathrm{GWN\text{-}S}} = M_8 \oplus \mathrm{ID}_i$。$A$ 访问每个传感器节点则可以获取所有 SN_j 和 GWN 之间的共享秘密参数 $K_{\mathrm{GWN\text{-}S}}$ 以及 SID_j，进而发起步骤 2)～5) 所述攻击。

2) 用户欺骗攻击

① A 记录所有发往 GWN 的$\{M_2,M_4,M_5,M_6,M_7\}$，记录 GWN 发出的所有$\{M_8,M_9,M_{10},M_{11}\}$，对于某个 SN_j 收到的$\{M_8,M_9,M_{10},M_{11}\}$，计算$\mathrm{ID}'_i = K_{\mathrm{GWN\text{-}S}} \oplus M_8$，$r'_g = h(\mathrm{ID}_i \| K_{\mathrm{GWN\text{-}S}}) \oplus M_9$，$r'_i = r'_g \oplus M_{10}$。对于每一组 $\{M_2,M_4,M_5,M_6,M_7\}$，计算 $M'_1 = M_5 \oplus r'_i$，$M'_6 = h(\mathrm{ID}'_i \| r'_i) \oplus \mathrm{SID}_j$，$M'_7 = h(M'_1 \| \mathrm{SID}_j \| M_3 \| r'_i)$。若$M'_6 = M_6$ 且 $M'_7 = M_7$，则该组 $\{M_8,M_9,M_{10},M_{11}\}$为用户 U_i 访问 SN_j 时所发送的消息，并且 GWN 发送的消息为当前验证的$\{M_8,M_9,M_{10},M_{11}\}$。

② A 通过如下方式伪造 GWN 的返回消息：选择随机数 r_j、r_g 计算$\mathrm{SK}_{\mathrm{GWN}} = h(\mathrm{ID}'_i \| \mathrm{SID}_j \| r'_i \| r_g \| r_j)$，$M_{14} = M'_1 \oplus r_g$，$M_{15} = r'_i \oplus r_j$，$M_{16} = h(\mathrm{ID}'_i \| \mathrm{SK}_{\mathrm{GWN}} \| r_g \| r_j)$。$A$ 发送$\{M_{14},M_{15},M_{16}\}$给 U_i。

③ 用户 U_i 收到 $\{M_{14},M_{15},M_{16}\}$后，计算 $r'_g = M_{14} \oplus M_1$，$r'_j = M_{15} \oplus r_i$，$\mathrm{SK}_i = h(\mathrm{ID}_i \| \mathrm{SID}_j \| r_i \| r'_g \| r'_j)$，$M'_{16} = h(\mathrm{ID}_i \| \mathrm{SK}_i \| r'_g \| r'_j)$。若 $M'_{16} = M_{16}$，则用户 U_i 接受此次 SK_i。

3) 用户伪装攻击

A 监听用户 U_i 和 SN_j 执行一轮完整协商，A 执行步骤①获取用户的 M_1、ID_i，执行如下过程伪造用户与 GWN 进行通信：A 选取随机数 s、r_i，计算 $M_2 = sP$，$M_3 = sX$，$M_4 = \mathrm{ID}_i \oplus M_3$，$M_5 = M_1 \oplus r_i$，$M_6 = h(\mathrm{ID}_i \| r_i) \oplus \mathrm{SID}_j$，$M_7 = h(M_1 \| \mathrm{SID}_j \| M_3 \| r_i)$，$A$ 发送 $\{M_2,M_4,M_5,M_6,M_7\}$给 GWN，GWN 验证后接受当

前消息并按照协议运行，则 A 伪装用户成功。

4) 前向安全问题

A 记录 GWN 发送给 SN_j 的所有 $\{M_8,M_9,M_{10},M_{11}\}$和 $\{M_{12},M_{13}\}$，计算 $ID_i=M_8\oplus K_{GWN\text{-}S}$，$r_g=h(ID_i\|K_{GWN\text{-}S})\oplus M_9$，$r_i=r_g\oplus M_{10}$，$r_j=M_{12}\oplus K_{GWN\text{-}S}$，$SK=h(ID_i\|SID_j\|r_i\|r_g\|r_j)$，则该协议不具备前向安全属性。

5) 离线字典猜测攻击

A 得到智能卡且通过恶意扫描器得到用户的生物特征 Bio_i，则可进行离线字典猜测攻击。A 执行步骤①获取用户的 ID_i，获取智能卡中的 A_i，从用户密码空间中猜测密码PW_i'并计算$c_i=f(\delta\oplus Bio_i)$，$A_i'=h(ID_i\|h(PW_i'\|a_i)\|c_i)$，其中 $f(\cdot)$对应表 1 中的 Rep(·) 函数，若$A_i'=A_i$则密码正确。故 A 可进行离线字典猜测攻击。

6) 内部攻击

A 在注册阶段得到用户发送的 RPW_i，并且攻击者得到用户智能卡中的 a_i，则攻击者可猜测 PW_i'，若$h(PW_i'\|a_i)=RPW_i$，则 A 猜中用户的密码，该攻击有效。

2.2 文献 [20] 协议的问题分析

KSSTI 攻击主要用于当计算 SK 的秘密参数仅只有临时秘密参数时，因此在协议设计时 SK 的参数需要同时具备长期秘密值和临时秘密值才可避免此类攻击。

1) 场景 1 的 KSSTI 攻击

① 场景 1 中，$SK=h(K_1\|K_3\|K_4\|SID_j^k)$，其中 $K_1=r_iP_k$，$K_3=r_jP_k$，$K_4=r_jK_1$。由于P_k,Y_k是系统参数，可通过智能卡获取，攻击者 A 在获得r_i,r_j临时秘密值后，进而可以计算出K_1,K_3,K_4。

② 通过公开信道得到 M_2, EID_j，其中 $M_2=ID_i^k\oplus h(K_1\|K_2)$，$EID_j=SID_j^k\oplus h(ID_i^k\|K_2)$，进而敌手可以进行如下计算$K_2=r_iY_k$，$ID_i^k=M_2\oplus h(K_1\|K_2)$，$SID_j^k=EID_j\oplus h(ID_i^k\|K_2)$。最终敌手 A 获得了 SK 的所有参数。

2) 场景 2 的 KSSTI 攻击

场景 2 中，$SK=h(K_4\|K_6\|K_7\|SID_j^2)$，其中$K_4=r_{12}P_2$，$K_7=r_jP_2$，由于$P_2,K_6,SID_j^2$可分别通过 MSG_4，MSG_8，MSG_2 获得，攻击者 A 在进一步获得r_i,r_j临时秘密值后，进而可以计算出K_4,K_7。最终敌手 A 获得了 SK 的所有参数。

3 提出新的协议

从前面的分析可看出，文献 [16] 的协议存在内部攻击、注册合法用户攻击、无前向安全性等缺点；文献 [20] 的协议存在 KSSTI 攻击，如果提出的认证协议能够实现以下 $G1$ 和 $G2$ 目标。$G1:SN_j|\equiv U_i \overset{sk}{\leftrightarrow} SN_j$，$G2:U_i|\equiv SN_j \overset{sk}{\leftrightarrow} U_i$，则表示正确地实现了相互认证与会话密钥协商。

本文将从以下 6 个方面着重考虑满足 S3、S4 中的离线字典攻击、KSSTI 攻击和 S9、S10 和 S11 标准的协议构建方法。

1) 更换存入智能卡中的随机数使协议满足 S3。

2) 智能卡对用户验证合法性时使用 Fuzzy-verifier 和 Honey words[25] 方法保证攻击者无法进行离线字典猜测攻击，也不能进行在线字典猜测攻击。

3) 向 SN_j 传递 U_i 秘密的相关信息，如下文协议中的 S_i；向 U_i 传递 SN_j 秘密的相关信息，如下文协议中的 S_j。可以看出 S_i, S_j 不能直接保证随机数暴露的情况下 SK 的安全性，进而抵抗 KSSTI 攻击。

4) 采用更换用户标识符的方法使协议满足 S9。

5) U_i 和 SN_j 之间利用 Diffie-Hellman 问题构建对称秘钥，使协议满足 S10。

6) GWN 和 SN_j 之间传递消息的验证秘密值随用户的不同而变化，以此防止注册用户攻击，使协议满足 S11，进而防止用户欺骗攻击和用户伪装攻击。

3.1 系统初始化

GWN 选定秘密值 X_{GWN}, $E(Fp)$, P, $h(\cdot)$，公开 $E(Fp)$, P, $h(\cdot)$，保存 X_{GWN}。

3.2 节点注册

GWN 为节点选定独特的 SID_j，计算$K_{GWN\text{-}S}=h(SID_j\|X_{GWN})$，在传感器节点中存储$\{SID_j, K_{GWN\text{-}S}\}$。

3.3 用户注册

如图 1 所示，用户输入 ID_i、PW_i、Bio_i，选择随机数 a、b'，计算：$Gen(Bio_i)=(\delta_i,\tau_i)$，$PID_i=h(ID_i\|\delta_i\|a)$，$RPW_i'=h(PW_i\|\delta_i\|b')$。$U_i\Rightarrow GWN:\{PID_i, RPW_i'\}$。

GWN 收到后计算$X_i=h(PID_i\|X_{GWN})$，$B_i'=X_i\oplus h(RPW_i'\|PID_i)$。GWN 在数据库中存入 $\{PID_i, Honey\_List=0\}$。$GWN\Rightarrow U_i$：智能卡$SC_i:\{B_i'\}$。

用户计算$X_i=B_i'\oplus h(RPW_i'\|PID_i)$。选择随机数 b，计算$RPW_i=h(PW_i\|\delta_i\|b)$，$B_i=X_i\oplus h(RPW_i\|PID_i)$，fuzzy-verifier: $A_i=h(PID_i\|RPW_i)\bmod n_0$，$n_0$ 为 $[2^6-2^8]$ 的整数，然后向智能卡 SC_i 中写入：a、b、B_i、A_i、P。

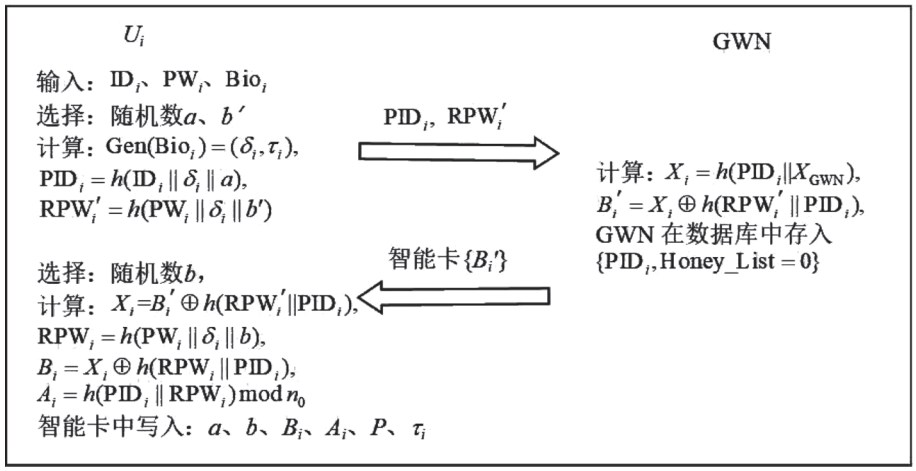

图 1　用户注册

3.4　用户登录及认证

如图 2 所示，用户输入 ID_i、PW_i、Bio_i。智能卡计算$\delta_i^*=\mathrm{Rep}(Bio_i,\tau_i)$，$PID_i^*=h(ID_i\|\delta_i^*\|a)$，$RPW_i^*=h(PW_i\|\delta_i^*\|b)$，$A_i^*=h(PID_i^*\|RPW_i^*)\bmod n_0$。比较$A_i^*?=A_i$，相等则继续，否则终止。计算$X_i=B_i\oplus h(RPW_i^*\|PID_i^*)$。选择随机数 a_{new}、r_i，计算$M_1=r_iP$，$PID_{new}=h(ID\|\delta_i^*\|a_{new})$，$M_2=h(M_1\|X_i)\oplus(PID_{new}\|SID_j)$，$M_3=h(X_i\|PID_{new}\|SID_j)$。$U_i\rightarrow GWN:\{PID_j,M_1,M_2,M_3\}$。

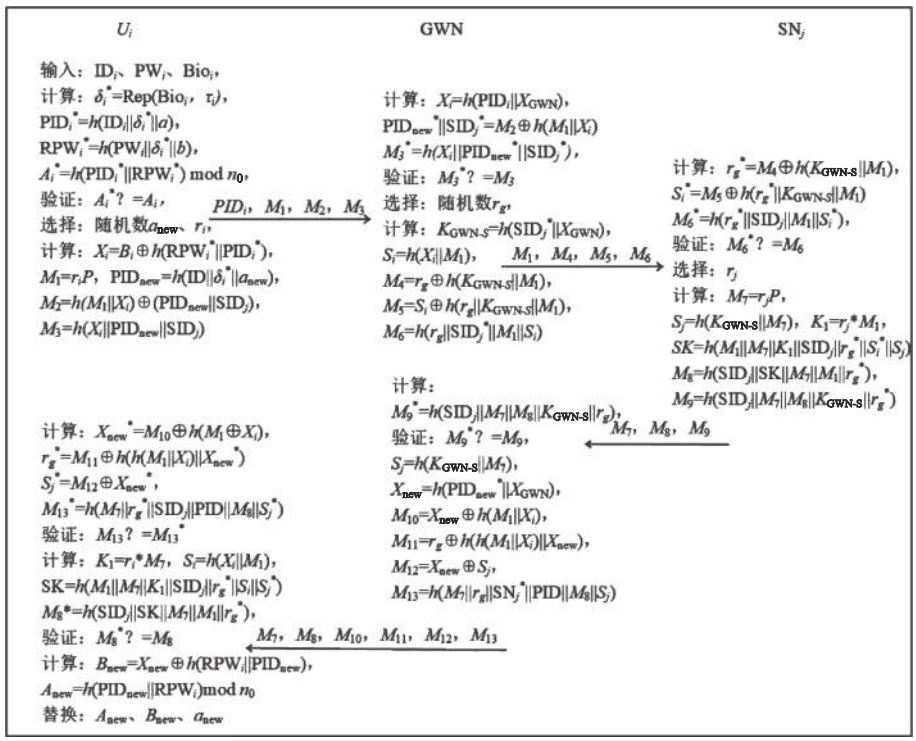

图 2　用户登录及认证

GWN 收到后计算 $X_i=h(PID_i\|X_{GWN})$，$PID_{new}^*\|SID_j^*=M_2\oplus h(M_1\|X_i)$，$M_3^*=h(X_i\|PID_{new}^*\|SID_j^*)$，比较 $M_3^*?=M_3$：1) 若不成立，结束会话，令 Honey_List = Honey_List + 1。若 Honey_List 大于阈值，则冻结用户，用户必须重新注册。2) 若成立，令 Honey_List = 0。GWN 选择随机数 r_g，计算 $K_{GWN\text{-}S}=h(SID_j^*\|X_{GWN})$，$S_i=h(X_i\|M_1)$，$M_4=r_g\oplus h(K_{GWN\text{-}S}\|M_1)$，$M_5=S_i\oplus h(r_g\|K_{GWN\text{-}S}\|M_1)$，$M_6=h(r_g\|SID_j^*\|M_1\|S_i)$。$GWN\rightarrow SN_j:\{M_1,M_4,M_5,M_6\}$。

SN_j 收到后，计算 $r_g^*=M_4\oplus h(K_{GWN\text{-}S}\|M_1)$，$S_i^*=M_5\oplus h(r_g^*\|K_{GWN\text{-}S}\|M_1)$，$M_6^*=h(r_g^*\|SID_j\|M_1\|S_i^*)$，比较 $M_6^*?=M_6$，不相等则拒绝，否则继续。SN_j 选择 r_j，计算 $M_7=r_jP$，$S_j=h(K_{GWN\text{-}S}\|M_7)$，$K_1=r_j^*M_1$，$SK=h(M_1\|M_7\|K_1\|SID_j\|r_g^*\|S_i^*\|S_j)$，$M_8=h(SID_j\|SK\|$

$M_7\|M_1\|r_g^*$)，$M_9=h(\mathrm{SID}_j\|M_7\|M_8\|K_{\mathrm{GWN\text{-}}S}\|r_g^*)$，$\mathrm{SN}_j\rightarrow$ GWN:{ M_7,M_8,M_9}。

GWN 计算$M_9^*=h(\mathrm{SID}_j^*\|M_7\|M_8\|K_{\mathrm{GWN\text{-}}S}\|r_g)$，比较$M_9^*?=M_9$，不相等则终止，否则继续。计算$S_j=h(K_{\mathrm{GWN\text{-}}S}\|M_7)$，$X_{\mathrm{new}}=h(\mathrm{PID}_{\mathrm{new}}{}^*\|X_{\mathrm{GWN}}\|)$，$M_{10}=X_{\mathrm{new}}\oplus h(M_1\|X_i)$，$M_{11}=r_g\oplus h(h(M_1\|X_i)\|X_{\mathrm{new}})$，$M_{12}=X_{\mathrm{new}}\oplus S_j$，$M_{13}=h(M_7\|r_g\|\mathrm{SID}_j^*\|\mathrm{PID}\|M_8\|S_j)$。用$\mathrm{PID}_{\mathrm{new}}{}^*$替换数据库中的$\mathrm{PID}_i$，将错误次数置零。GWN $\rightarrow U_i$:{$M_7,M_8,M_{10},M_{11},M_{12},M_{13}$}。

U_i 计算$X_{\mathrm{new}}{}^*=M_{10}\oplus h(M_1\oplus X_i)$，$r_g^*=M_{11}\oplus h(h(M_1\|X_i)\|X_{\mathrm{new}}{}^*)$,$S_j{}^*=M_{12}\oplus X_{\mathrm{new}}{}^*$,$M_{13}^*=h(M_7\|r_g^*\|\mathrm{SID}_j\|\mathrm{PID}\|M_8\|S_j^*)$，比较$M_{13}?=M_{13}^*$，相等则进行下列计算：$K_1=r_i^*M_7$，$S_i=h(X_i\|M_1)$，$\mathrm{SK}=h(M_1\|M_7\|K_1\|\mathrm{SID}_j\|r_g^*\|S_i\|S_j^*)$，$M_8^*=h(\mathrm{SID}_j\|\mathrm{SK}\|M_7\|M_1\|r_g^*)$，比较$M_8^*?=M_8$，相等则进行下列计算：$B_{\mathrm{new}}=X_{\mathrm{new}}\oplus h(\mathrm{RPW}_i\|\mathrm{PID}_{\mathrm{new}})$，$A_{\mathrm{new}}=h(\mathrm{PID}_{\mathrm{new}}\|\mathrm{RPW}_i)\bmod n_0$，用$A_{\mathrm{new}}$、$B_{\mathrm{new}}$、$a_{\mathrm{new}}$替换智能卡中的$A_i$、$B_i$、$a$。

3.5 更改密码

用户输入 ID_i、PW_i、Bio_i。智能卡计算$\delta_i{}^*=\mathrm{Rep}(\mathrm{Bio}_i,\tau_i)$，$\mathrm{PID}_i{}^*=h(\mathrm{ID}_i{}^*\|\delta_i{}^*\|a)$，$\mathrm{RPW}_i{}^*=h(\mathrm{PW}_i{}^*\|\delta_i{}^*\|b)$，$A_i{}^*=h(\mathrm{PID}_i{}^*\|\mathrm{RPW}_i{}^*)\bmod n_0$。比较$A_i{}^*?=A_i$，相等则继续，否则终止。输入新的密码$\mathrm{PW}_{\mathrm{new}}$，选择新的随机数$b_{\mathrm{new}}$，计算$\mathrm{RPW}_{\mathrm{new}}=h(\mathrm{ID}_i,\delta_i{}^*,a)$，$A_{\mathrm{new}}=h(\mathrm{PID}_i{}^*\|\mathrm{RPW}_{\mathrm{new}})\bmod n_0$，$B_{\mathrm{new}}=B_i\oplus h(\mathrm{RPW}_{\mathrm{new}}\|\mathrm{PID})$，用$A_{\mathrm{new}}$、$B_{\mathrm{new}}$、$b_{\mathrm{new}}$替换$A_i$、$B_i$、$b$。$A_{\mathrm{new}}=h(\mathrm{PID}_i{}^*\|\mathrm{RPW}_{\mathrm{new}})\bmod n_0$，$B_{\mathrm{new}}=B_i\oplus h(\mathrm{RPW}_{\mathrm{new}}\|\mathrm{PID})$，用$A_{\mathrm{new}}$、$B_{\mathrm{new}}$、$b_{\mathrm{new}}$替换$A_i$、$B_i$、$b$。

4 形式化安全性分析

本节将用 BAN 逻辑对协议正确性进行验证。协议的正确性指的是协议执行完后，用户U_i和传感器节点SN_j共享一个新鲜的会话密钥 SK。BAN 逻辑用到的符号和规则定义如表 2 所示。为了便于使用 BAN 逻辑对协议进行分析，现将协议的消息理想化为如下消息。

表 2 BAN 逻辑符号及规则

符号及规则	描述	符号及规则	描述	符号及规则	描述
$P\|\equiv X$	P相信X	$<X>_Y$	X和Y结合	$P\|\sim Q$	P曾经说过X
$P\triangleleft X$	P收到X	$\{X\}_Y$	X用秘钥K加密	$P\|\Rightarrow X$	P对X有控制权
$P\overset{\mathrm{SK}}{\leftrightarrow}Q$	P和Q通过秘钥SK进行通信	$\dfrac{P\|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P\|\equiv Q\|\sim X}$	R1：消息含义规则	$\dfrac{P\|\equiv\#(X),P\|\equiv Q\|\sim X}{P\|\equiv Q\equiv X}$	R2：随机数验证规则
$\#(X)$	X是新鲜的	$\dfrac{P\|\equiv Q\|\equiv X,P\|\equiv Q\|\Rightarrow X}{P\|\equiv X}$	R3：仲裁规则	$\dfrac{P\|\equiv\#(X)}{P\|\equiv\#(X,Y)}$	R4：新鲜性规则
$\dfrac{P\|\equiv(X,Y)}{P\|\equiv X}$	R5：信念规则	$\dfrac{P\|\equiv\#(X),P\|\equiv Q\|\equiv X}{P\|\equiv P\overset{\mathrm{SK}}{\leftrightarrow}Q}$	R6：会话秘钥规则		

1) 消息 1：$U_i\rightarrow$GWN:$\mathrm{PID}_i,M_1,M_2,M_3:<M_1,\mathrm{SID}_j>X_{U_i}$

2) 消息 2：GWN$\rightarrow\mathrm{SN}_j$:$M_1,M_4,M_5,M_6:<r_g,\mathrm{SID}_j,U_i|\equiv M_1>K_{\mathrm{GWN\text{-}}S}$

3) 消息 3：$\mathrm{SN}_j\rightarrow$ GWN : $M_7,M_8,M_9:<\mathrm{SID}_j,M_7,r_g>K_{\mathrm{GWN\text{-}}S}$

4) 消息 4：GWN$\rightarrow U_i:M_7,M_8,M_9,M_{10},M_{11},M_{12},M_{13}:<\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j|\equiv M_7,r_g>X_{U_i}$

根据 3.4 节协议内容初始化假设：

A1：$\mathrm{GWN}|\equiv U_i\overset{X_{U_i}}{\longleftrightarrow}\mathrm{GWN}$

A2：$\mathrm{GWN}|\equiv\#(M_1)$

A3：$\mathrm{GWN}|\equiv U_i|\Rightarrow<M_1,\mathrm{SID}_j>$

A4：$\mathrm{SN}_j|\equiv\mathrm{GWN}\overset{K_{\mathrm{GWN\text{-}}S}}{\longleftrightarrow}\mathrm{SN}_j$

A5：$\mathrm{SN}_j|\equiv\#(M_1)$

A6：$\mathrm{SN}_j|\equiv\mathrm{GWN}|\Rightarrow<r_g,\mathrm{SID}_j,U_i|\equiv M_1>$

A7：$\mathrm{SN}_j|\equiv U_i|\Rightarrow U_i\overset{\mathrm{SK}}{\longleftrightarrow}\mathrm{SN}_j$

A8：$\mathrm{GWN}|\equiv\mathrm{GWN}\overset{K_{\mathrm{GWN\text{-}}S}}{\longleftrightarrow}\mathrm{SN}_j$

A9：$\mathrm{GWN}|\equiv\#(M_7)$

A10：$U_i|\equiv U_i\overset{X_{U_i}}{\longleftrightarrow}\mathrm{GWN}$

A11：$U_i|\equiv\#(M_7)$

A12：$U_i|\equiv\mathrm{GWN}|\Rightarrow<\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j|\equiv M_7,r_g>$

A13：$U_i|\equiv\mathrm{SN}_j|\Rightarrow U_i\overset{\mathrm{SK}}{\longleftrightarrow}\mathrm{SN}_j$

如果提出的认证协议能够实现以下目标，那么所提协议正确实现了相互认证与会话密钥协商。

G1：$\mathrm{SN}_j|\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}\mathrm{SN}_j$

G2：$U_i|\equiv\mathrm{SN}_j\overset{\mathrm{SK}}{\longleftrightarrow}U_i$

BAN 逻辑形式化分析如下。

从消息 1，得到：

$$\mathrm{GWN}\triangleleft<M_1,\mathrm{SID}_j>_{X_{U_i}} \tag{1}$$

根据式 (1)、A1、应用消息含义规则，得到：

$$\mathrm{GWN}|\equiv U_i|\sim <M_1,\mathrm{SID}_j> \tag{2}$$

根据式 (2)、A2、应用随机数验证规则，得到：

$$\mathrm{GWN}|\equiv U_i|\equiv <M_1,\mathrm{SID}_j> \tag{3}$$

根据式 (3)、A3、应用仲裁规则，得到：

$$\mathrm{GWN}|\equiv <M_1,\mathrm{SID}_j> \tag{4}$$

从消息 2，得到：

$$\mathrm{SN}_j\triangleleft <r_g,\mathrm{SID}_j,U_i|\equiv M_1>_{K_{\mathrm{GWN}\text{-}S}} \tag{5}$$

根据式 (5)、A4、应用消息含义规则，得到：

$$\mathrm{SN}_j|\equiv \mathrm{GWN}|\sim <r_g,\mathrm{SID}_j,U_i|\equiv M_1> \tag{6}$$

根据式 (6)、A5、应用随机数验证规则，得到：

$$\mathrm{SN}_j|\equiv \mathrm{GWN}|\equiv <r_g,\mathrm{SID}_j,U_i|\equiv M_1> \tag{7}$$

根据式 (7)、A6、应用仲裁规则，得到：

$$\mathrm{SN}_j|\equiv <r_g,\mathrm{SID}_j,U_i|\equiv M_1> \tag{8}$$

根据式 (8)、应用信念规则，得到：

$$\mathrm{SN}_j|\equiv U_i|\equiv M_1 \tag{9}$$

根据式 (9)、$\mathrm{SK}=h(M_1\|M_7\|r_j{}^*M_1\|\mathrm{SN}_j\|r_g\|S_i\|S_j)$、应用会话秘钥规则，得到：

$$\text{目标}(G1)：\mathrm{SN}_j|\equiv U_i\overset{\mathrm{SK}}{\longleftrightarrow}\mathrm{SN}_j \tag{10}$$

从消息 3，得到：

$$\mathrm{GWN}\triangleleft <\mathrm{SID}_j,M_7,r_g>K_{\mathrm{GWN}\text{-}S} \tag{11}$$

根据式 (11)、A8、应用消息含义规则，得到：

$$\mathrm{GWN}\left|\equiv \mathrm{SN}_j\right|\sim <\mathrm{SID}_j,M_7,r_g> \tag{12}$$

根据式 (12)、A9、应用随机数验证规则，得到：

$$\mathrm{GWN}\left|\equiv \mathrm{SN}_j\right|\equiv <\mathrm{SID}_j,M_7,r_g> \tag{13}$$

根据式 (13)、A10、应用仲裁规则，得到：

$$\mathrm{GWN}|\equiv <\mathrm{SID}_j,M_7,r_g> \tag{14}$$

从消息 4，得到：

$$U_i\triangleleft <\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j|\equiv M_7,r_g>X_{U_i} \tag{15}$$

根据式 (15)、A10、应用消息含义规则，得到：

$$U_i|\equiv \mathrm{GWN}|\sim <\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j|\equiv M_7,r_g> \tag{16}$$

根据式 (16)、A11、应用随机数验证规则，得到：

$$U_i|\equiv \mathrm{GWN}|\equiv <\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j|\equiv M_7,r_g> \tag{17}$$

根据式 (17)、A12、应用仲裁规则，得到：

$$U_i\left|\equiv <\mathrm{SID}_j,\mathrm{SN}_j|\equiv M_1,\mathrm{SN}_j\right|\equiv M_7,r_g> \tag{18}$$

根据式 (18)，应用信念规则，得到：

$$U_i\left|\equiv \mathrm{SN}_j|\equiv M_1,U_i\right|\equiv \mathrm{SN}_j|\equiv M_7 \tag{19}$$

根据式 (19)、$\mathrm{SK}=h(M_1\|M_7\|K_1\|\mathrm{SID}_j\|r_g\|S_i\|S_j)$、应用会话秘钥规则，得到：

$$\text{目标}(G2)：U_i|\equiv \mathrm{SN}_j\overset{\mathrm{SK}}{\longleftrightarrow}U_i \tag{20}$$

从式 (10) 和式 (20) 可以看出该文协议满足安全目标，用户 U_i 和传感器节点 SN_j 都相信彼此之间共享一个新鲜的会话密钥 SK。

5　非形式化安全性分析

5.1　用户匿名性

用户匿名性要求攻击者无法根据交互信息得到用户的 ID 或无法从多个会话中分析出属于某个用户产生的会话。用户和 SN_j 协商过程产生的交互信息和用户 ID 相关的消息为 PID 和 M_2，攻击者在缺少 X_i 的情况下无法从 M_2 中解析出 $\mathrm{PID}_{\mathrm{new}}$，故无法通过 $\mathrm{PID}_{\mathrm{new}}$ 解析 ID 的相关信息。由于单向函数 h 的存在，攻击者在得到 PID 后无法反向解析出 ID 等信息。另一方面，攻击者在一次会话中能监听到用户当前所用 PID，但在缺少 X_i 的情况下，无法解析用户下次使用的 $\mathrm{PID}_{\mathrm{new}}$，故攻击者无法分辨同一用户使用的两次 PID。故本协议具有用户匿名性。

5.2　前向安全

本协议基于 DH 问题设计用户和 SN_j 的对称秘钥产生过程。本协议中 $\mathrm{SK}=h(M_1\|M_7\|K_1\|\mathrm{SID}_j\|r_g\|S_i\|S_j)$，攻击者在得到所有长期秘密后，可以解析出 M_1、M_7、SID_j、r_g、S_i、S_j 信息。由于存在 Diffie-Hellman 问题，在缺少临时秘密 r_i 和 r_j 的情况下，攻击者无法计算出 K_1。由于单向哈希函数 h 的存在，在不知道 K_1 的情况下无法解析 SK，故本协议具有前向安全属性。

5.3　离线字典攻击

攻击者在得到智能卡和用户生物信息后，从用户身份空间 D_{ID} 和用户密码空间 D_{PW} 中猜测 $(\mathrm{ID}^*,\mathrm{PW}^*)$，计算 $\delta_i^*=\mathrm{Rep}(\mathrm{Bio}_i,\tau_i)$，$\mathrm{PID}_i^*=h(\mathrm{ID}_i^*\|\delta_i^*\|a)$，$\mathrm{RPW}_i^*=h(\mathrm{PW}_i^*\|\delta_i^*\|b)$，$A_i^*=h(\mathrm{PID}_i^*\|\mathrm{RPW}_i^*)\bmod n_0$。通过比较 A_i^* 与 A_i 是否相等判断猜测的 PW 和 ID 是否正确。假设 $|D_{\mathrm{ID}}|=|D_{\mathrm{PW}}|=10^6$，$n_0=2^8$，则符合该等式的 $(\mathrm{ID}^*,\mathrm{PW}^*)$ 对有 $\frac{|D_{\mathrm{ID}}|*|D_{\mathrm{PW}}|}{n_0}\approx 2^{32}$ 个，攻击者只能采取线上同 GWN 交互的方式确认此次猜测的 $(\mathrm{ID}^*,\mathrm{PW}^*)$ 是否正确，但由于 GWN 用户校验次数 Honey_List 不能超过阈值，故在有限次的线上猜测过程中，猜对用户的身份和密码的概率可以忽略，故本协议能抵御离线字典攻击。

5.4 内部攻击

攻击者在注册阶段得到用户的 $(\mathrm{PID}_i,\mathrm{RPW}_i')$，若攻击者又获得了用户的智能卡以及生物特征 Bio_i，则只能通过 RPW_i'猜测用户的密码。攻击者在密码空间 D_{PW} 中猜测 PW^*后，通过计算 $\delta_i=\mathrm{Rep}(\mathrm{Bio}_i,\tau_i)$，$\mathrm{RPW}_i'=h(\mathrm{PW}_i\|\delta_i\|b')$，验证 PW^*猜测是否正确。由于智能卡在注册完成后，已将 b'替换成了 b，使攻击者无法通过智能卡得到 b'，也不能通过 RPW_i'猜测用户的密码，故本协议能抵御内部攻击。

5.5 KSSTI 攻击

在该攻击中，攻击者得到用于产生会话秘钥 SK 的所有随机秘密。在本协议中，攻击者能得到 r_g、r_i、r_j，可监听通信过程中的所有消息。用户和 SN_j 产生的 $\mathrm{SK}=h(M_1\|M_7\|K_1\|\mathrm{SID}_i\|r_g\|S_i\|S_j)$，通过计算或监听得到 M_1、M_7、K_1，但计算 S_i 的途径只有两个：直接通过 $S_i=h(X_i\|M_1)$计算，但攻击者缺少 X_i，故此种计算方法不可行；通过 $S_i=M_5\oplus h(r_g\|K_{\mathrm{GWN}\text{-}S}\|M_1)$计算，但缺少 $K_{\mathrm{GWN}\text{-}S}$ 的情况下也无法计算 S_i。故攻击者无法计算出 S_i。同理，攻击者也无法计算出 S_j、SID_j。由于单向哈希函数 h 的存在，攻击者在缺少 S_i、S_j、SID_j 的情况下无法计算本次协商的会话秘钥 SK，故本协议能抵抗 KSSTI 攻击。

5.6 注册合法用户攻击

在该攻击中，攻击者通过注册合法用户访问传感器节点的方法试图破解其他用户和该传感器节点协商的秘钥或其他有用信息，该种攻击是否有效主要看攻击者能否通过协商获取 GWN 和 SN_j 之间认证的秘密的相关信息。在本协议中，攻击者注册成合法用户，同 SN_j 协商后，获得当前合法用户所能得到的消息 (如 r_g)，并窃听信道传输的内容 (如 M_4)，计算$h(K_{\mathrm{GWN}\text{-}S}\|M_1)=M_4\oplus r_g$，但由于单向哈希函数 h 的存在无法进一步计算出 $K_{\mathrm{GWN}\text{-}S}$。本协议中，每次协商 $K_{\mathrm{GWN}\text{-}S}$ 连接用户产生的临时消息 M_1 后，通过哈希函数产生加密消息的秘钥，故不同的用户协商过程中，GWN 用以加密和 SN_j 之间秘密的秘钥 $h(K_{\mathrm{GWN}\text{-}S}\|M_1)$ 是不同的，攻击者无法通过此种攻击计算出任何能破解其他合法用户协商的有用信息，故本协议能够抵抗注册合法用户攻击。

6 与相关协议的对比分析

从安全性和性能两方面对相关协议进行对比分析，结果如表 3 和表 4 所示。表 3 对比了几种相关协议的安全性，“是”表示能够满足对应的安全属性或者能够抵抗对应的攻击，可以看出该文协议能够克服已有文献的安全风险。表 4 进行了计算量和通信量的对比，其中将该文协议与对比协议所使用的各参数长度及密码学原语进行如下统一：时间戳和身份标识的比特串长度均为 128 bit，哈希原语为 SHA-128(记为 T_h)、椭圆曲线标量乘原语为 ECC-160(记为 T_m)、生物特征恢复函数原语为 Rep(.)[26](记为 T_R)、对称加解密为 AES-128(记为 T_S)。在进行计算量对比时，⊕和||操作时间忽略不计，上述原语 T_h、T_m、T_R、T_S 在 1 024 MB RAM 的 Intel Pentium4 2 600 MHz 处理器上执行一次所花费的时间为T_h=0.5ms、T_m=63.08ms、$T_R\approx T_m$、T_S=8.7ms[27-28]。经过对比表明，该文协议在保证更高安全等级的同时，计算量与其他协议相比适中，这是因为协议使用了椭圆曲线标量乘，而椭圆曲线标量乘的计算开销要明显高于哈希运算及对称加密。此外，在通信量上与其他协议相比适中。

表 3 相关协议安全性对比分析

协议	发表年份/年	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
文献[18]	2019	是	是	是	否	是	是	否	是	是	是	是
文献[14]	2018	是	是	否	否	是	是	否	是	是	否	是
文献[16]	2018	是	是	否	否	是	是	是	是	是	否	否
文献[15]	2018	否	是	否	否	是	否	否	是	是	否	是
文献[20]	2020	是	是	是	否	是	是	是	是	是	是	是
文献[11]	2017	是	是	否	否	是	是	否	是	否	否	是
文献[22]	2017	否	是	否	否	是	是	否	是	否	否	是
文献[21]	2018	是	是	否	否	是	是	否	是	否	否	否
该文协议	2022	**是**	**是**	**是**	**是**	**是**	**是**	**是**	**是**	**是**	**是**	**是**

表 4　相关协议性能对比

协议	计算量/s				通信量/bit				
	U_i	GWN	SN_j	总计算量	总时间/ms	U_i	GWN	SN_j	总通信量/bit
文献[18]	$12T_h+2T_m+T_R$	$10T_h+T_s$	$5T_h+2T_m+T_s$	$27T_h+4T_m+2T_s+T_R$	346.3	1056	1472	544	3072
文献[14]	$9T_h+1T_s+T_R$	$3T_h+2T_s$	$2T_h+T_s$	$14T_h+4T_s+T_R$	104.88	512	896	384	1792
文献[16]	$8T_h+2T_m+T_R$	$9T_h+T_m$	$4T_h$	$21T_h+3T_m+T_R$	262.82	704	896	256	1856
文献[15]	$9T_h$	$15T_h$	$9T_h$	$33T_h$	16.5	640	1280	1792	3712
文献[20]	$8T_h+3T_m+T_R$	$9T_h+T_m$	$4T_h+2T_m$	$21T_h+6T_m+T_R$	452.56	544	704	288	1536
文献[11]	$8T_h+T_s$	$5T_h+2T_s$	$5T_h+T_s$	$18T_h+4T_s$	43.8	512	768	512	1792
文献[22]	$9T_h+T_R$	$14T_h$	$7T_h$	$30T_h+T_R$	78.08	640	1280	384	2304
文献[21]	$7T_h+2T_s+T_R$	$7T_h+3T_s$	$4T_h+T_s$	$18T_h+6T_s+T_R$	124.28	896	1664	384	2944
该文协议	$14T_h+2T_m+T_R$	$13T_h$	$7T_h+2T_m$	$34T_h+4T_m+T_R$	332.4	672	1344	416	2432

7　结 束 语

本文指出文献 [16] 协议不能抵抗合法用户攻击、用户欺骗攻击、用户伪装攻击、离线字典攻击等安全性问题。为确保高安全场景下 WSN 的安全通信，该文将 KSSTI 攻击和注册合法用户攻击加入安全模型，提出了一种三因素安全增强身份认证协议，实现了用户和传感器节点两端的安全会话密钥协商。最后采用了 BAN 逻辑和非形式化分析的方法对所提协议进行安全分析，结果表明本文协议能够满足该增强安全模型中的所有评价标准。与已有相关文献相比，本文给出的增强安全模型安全等级更高。此外，本文协议计算量和通信量适中，适合应用在对安全等级要求更高的场景中。

参　考　文　献

[1] ABI-CHAR P E, NADER P, MAHFOUZ S. A secure and lightweight authenticated key agreement protocol for distributed IoT applications[C]//2020 43rd International Conference on Telecommunications and Signal Processing (TSP). [S.l.]: IEEE, 2020: 50-56.

[2] KANDRIS D, NAKAS C, VOMVAS D, et al. Applications of wireless sensor networks: An up-to-date survey[J]. Applied System Innovation, 2020, 3(1): 14.

[3] VINOTH R, DEBORAH L J, VIJAYAKUMAR P, et al. Secure multifactor authenticated key agreement scheme for industrial IoT[J]. IEEE Internet of Things Journal, 2020, 8(5): 3801-3811.

[4] MAJID M, HABIB S, JAVED A R, et al. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review[J]. Sensors, 2022, 22(6): 2087.

[5] ZHANG K, XU K, WEI F. A provably secure anonymous authenticated key exchange protocol based on ECC for wireless sensor networks[J]. Wireless Communications and Mobile Computing, 2018, DOI: 10.1155/2018/2484268.

[6] WANG C, WANG D, TU Y, et al. Understanding node capture attacks in user authentication schemes for wireless sensor networks[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 19(1): 507-523.

[7] CHANG T Y, HWANG M S, YANG W P. A communication-efficient three-party password authenticated key exchange protocol[J]. Information Sciences, 2011, 181(1): 217-226.

[8] CHANDER B, KUMARAVELAN G. An improved 2-factor authentication scheme for WSN based on ECC[J]. IETE Technical Review, 2022, 40(2): 1-12.

[9] ZHU L, XIANG H, ZHANG K. A light and anonymous three-factor authentication protocol for wireless sensor networks[J]. Symmetry, 2021, 14(1): 46.

[10] SHIN S H, KOBARA K. Security analysis of password-authenticated key retrieval[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14: 573-576.

[11] MIR O, MUNILLA J, KUMARI S. Efficient anonymous authentication with key agreement protocol for wireless Medical sensor networks[J]. Peer-to-Peer Networking and Applications, 2017, 10(1): 79-91.

[12] HE D, KUMAR N, CHEN J, et al. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks[J]. Multimedia Systems, 2015, 21(1): 49-60.

[13] 李文婷, 汪定, 王平, 等. 无线传感器网络下多因素身份认证协议的内部人员攻击[J]. 软件学报, 2019, 30(8): 2375-2391.
LI W T, WANG D, WANG P, et al. Insider attacks against multi-factor authentication protocols for wireless sensor networks[J]. Journal of Software, 2019, 30(8): 2375-2391.

[14] 房卫东, 张武雄, 杨旸, 等. 基于生物特征标识的无线传感器网络三因素用户认证协议[J]. 电子学报, 2018, 46(3): 702-713.
FANG W D, ZHANG W X, YANG Y, et al. BTh-UAP: Biometric-Based three-factor user authentication protocol for wireless sensor network[J]. Acta Electronica Sinica, 2018, 46(3): 702-713.

[15] AMIN R, ISLAM S K H, BISWAS G P, et al. A robust mutual authentication protocol for WSN with multiple base-stations[J]. Ad Hoc Networks, 2018, 75: 1-18.

[16] LI X, NIU J, KUMARI S, et al. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments[J]. Journal of Network and Computer Applications, 2018, 103: 194-204.

[17] JIANG Q, MA J, WEI F, et al. An untraceable

teMporalcredential-based two-factor authentication scheMe using ecc for wireless sensor networks[J]. Journal Of Network And Computer Applications, 2016, 76: 37-48.

[18] MO J, CHEN H. A lightweight secure user authentication and key agreement protocol for wireless sensor networks[J]. Security and Communication Networks, 2019, 2019: 1-17.

[19] LU Y, XU G, LI L, et al. Anonymous three-factor authenticated key agreement for wireless sensor networks[J]. Wireless Networks, 2019, 25(4): 1461-1475.

[20] 王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683-700.
WANG C Y, WANG D, WANG F F, et al. Multi-Factor user authentication scheme for multi-gateway wireless sensor networks[J]. Chinese Journal of Computers, 2020, 43(4): 683-700.

[21] ALI R, PAL A K, KUMARI S, et al. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring[J]. Future Generation Computer Systems, 2018, 84: 200-215.

[22] SRINIVAS J, MUKHOPADHYAY S, MISHRA D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks[J]. Ad Hoc Networks, 2017, 54: 147-169.

[23] XUE L, HUANG Q, ZHANG S, et al. A lightweight three-factor authentication and key agreement scheme for multigateway WSNs in IoT[J]. Security and Communication Networks, 2021(4): 1-15.

[24] GUO H, GAO Y, XU T, et al. A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks[J]. Ad Hoc Networks, 2019, 95: 101965.1-101965.16.

[25] WANG D, WANG P. Two birds with one stone: Two-Factor authentication with security beyond conventional bound[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(4): 708-722.

[26] DODIS Y, REYZIN L, SMITH A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Heidelberg: Springer, 2004: 523-540.

[27] KOCAREV L. Chaos-Based cryptography: Theory, algorithms and applications[M]. Berlin/Heidelberg: Springer Science & Business Media, 2011.

[28] BRUCE S. Applied cryptography: Protocols, algorthms, and source code in C[M]. 2nd. Hoboken: John Wiley & Sons, Inc, 1996.

编 辑 叶 芳