面向多网关的无线传感器网络多因素认证协议

王晨宇[1)] 汪 定[2),3)] 王菲菲[1)] 徐国爱[1)]

[1)](北京邮电大学网络空间安全学院 北京 100876)

[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)

摘 要 无线传感器网络作为物联网的重要组成部分,广泛应用于环境监测、医疗健康、智能家居等领域.身份认证为用户安全地访问传感器节点中的实时数据提供了基本安全保障,是保障无线传感器网络安全的第一道防线;前向安全性属于系统安全的最后一道防线,能够极大程度地降低系统被攻破后的损失,因此一直被学术及工业界视为重要的安全属性.设计面向多网关的可实现前向安全性的无线传感器网络多因素身份认证协议是近年来安全协议领域的研究热点.由于多网关无线传感器网络身份认证协议往往应用于高安全需求场景,一方面需要面临强大的攻击者,另一方面传感器节点的计算和存储资源却十分有限,这给如何设计一个安全的多网关无线传感器网络身份认证协议带来了挑战.近年来,大量的多网关身份认证协议被提出,但大部分都随后被指出存在各种安全问题.2018年,Ali等人提出了一个适用于农业监测的多因素认证协议,该协议通过一个可信的中心(基站)来实现用户与外部的传感器节点的认证;Srinivas等人提出了一个通用的面向多网关的多因素身份认证协议,该协议不需要一个可信的中心,而是通过在网关之间存储共享秘密参数来完成用户与外部传感器节点的认证.这两个协议是多网关无线传感器网络身份认证协议的典型代表,分别代表了两类实现不同网关间认证的方式:1)基于可信基站,2)基于共享秘密参数.分析指出这两个协议对离线字典猜测攻击、内部攻击是脆弱的,且无法实现匿名性和前向安全性.鉴于此,本文提出一个安全增强的可实现前向安全性的面向多网关的无线传感器网络多因素认证协议.该协议采用Srinivas等协议的认证方式,即通过网关之间的共享秘密参数完成用户与外部传感器节点的认证,包含两种典型的认证场景.对新协议进行了BAN逻辑分析及启发式分析,分析结果表明该协议实现了双向认证,且能够安全地协商会话密钥以及抵抗各类已知的攻击.与相关协议的对比结果显示,新协议在提高安全性的同时,保持了较高的效率,适于资源受限的无线传感器网络环境.

关键词 多网关的无线传感器网络;口令认证协议;离线口令猜测攻击;仿冒攻击;前向安全

中图法分类号 TP309.08 **DOI号** 10.11897/SP.J.1016.2020.00683

Multi-factor User Authentication Scheme for Multi-gateway Wireless Sensor Networks

WANG Chen-Yu[1)] WANG Ding[2),3)] WANG Fei-Fei[1)] XU Guo-Ai[1)]

[1)](*School of Cyber-security, Beijing University of Posts and Telecommunications, Beijing* 100876)

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

[3)](*National Engineering Laboratory of Mobile Network Security (Nankai University), Tianjin* 300350)

Abstract Wireless sensor networks, as a fundamental infrastructure of internet of things, have played an important role in security-critical applications, such as environmental monitoring, personas health and smart home. User authentication can guarantee that users securely access real-time data in sensor nodes, and it is the first line of defense to ensure the security of wireless sensor networks. In

收稿日期:2019-09-28;在线出版日期:2020-02-08.本课题得到国家重点研发计划No.2018YFB0803605、国家自然基金No.61802006资助.**王晨宇**,博士生,中国计算机学会(CCF)会员,主要研究领域为安全协议,E-mail:wangchenyu@bupt.edu.cn.**汪 定**(通信作者),教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为认证协议与口令安全,E-mail:wangding@nankai.edu.cn.**王菲菲**,博士生,主要研究领域为安全协议.**徐国爱**,教授,博士生导师,研究领域为信息安全与软件安全.

addition, forward security can be regarded as the last line of defense for the security of systems, which can greatly reduce the loss of information security after the system is compromised. Therefore, it has been regarded as an important security attribute by academics and industry. The design of a multi-factor user authentication for multi-gateway wireless sensor networks has attracted intensive discussions in the field of security protocols. However, confronted with a powerful adversary, resource-constrained hardware and an impressive list of attributes, it is full of challenging in designing a secure user authentication scheme for multi-gateway wireless sensor networks. Recently, many multi-factor user authentication schemes for multi-gateway wireless sensor networks are proposed, but most of them are found insecure shortly. Specifically, most of them cannot resist smart card loss attacks, insider attacks and cannot achieve user anonymity and forward secrecy. In 2018, Ali et al. proposed a multi-factor user authentication scheme for agriculture monitoring under multi-gateway wireless sensor networks. In Ali et al.'s scheme, a trusted center (base station) is required to support the authentication between users and sensor nodes that are not connected to the home gateway. In the same year, Srinivas et al.'s also presented a multi-factor authentication for multi-gateway wireless sensor networks, their scheme does not need a trusted center, and it builds a shared secret key to finish the authentication between users and foreign sensor nodes. These two schemes are typical representatives of multi-factor user authentication schemes for multi-gateway wireless sensor networks, and they represent two types of authentication methods for the authentication between different gateways: 1) based on the trusted base station; 2) based on the shared secret parameters.

In this paper, we analyze these two recent typical user authentication schemes for multi-gateway wireless sensor networks, hoping to take these two schemes as study cases to identify the common weaknesses of user authentication schemes and providing corresponding specific solutions. We find that they both are vulnerable to offline-dictionary guessing attack, insider attack and fail to achieve forward secrecy and user anonymity. To overcome these weaknesses, we propose an enhanced multi-factor user authentication scheme for multi-gateway wireless sensor networks with forward secrecy. The proposed scheme adopts Srinivas et al.'s method and achieves the authentication between users and foreign sensor nodes by using a shared secret key among gateways, including two typical authentication scenarios. We prove that it achieves mutual authentication, provides secure session key agreement and can resist to know attacks via BAN logic and heuristic analysis. We compare it with several typical relevant user authentication schemes for multi-gateway wireless sensor networks from the security and performance. The results show that the proposed scheme provides better security for the applications of multi-gateway wireless sensor networks that have high security requirements, and thus it is more suitable to resource-constrained environments.

Keywords multi-gateway wireless sensor networks; password-based authentication protocol; offline-dictionary attack; impersonation attack; forward secrecy

1 引 言

无线传感器网络(Wireless Senor Networks, WSNs)是物联网感知周围环境、收集数据的关键组件,被广泛应用于智能家居[1]、公共安全[2]和医疗健康[3]等领域. WSNs由通过无线通信技术连接的大量传感器节点组成,这些传感器节点可以协作监控网络区域覆盖的信息,并允许外部合法用户访问传感器节点中的实时数据以获取监控实体的状态[4]. 传感器节点通常是低功耗的设备,配备一个或多个传感器、存储器、处理器、电源和执行器,可以随机部署到任何环境中,以实时检测环境,但受自身存储能力和计算能力的限制,处理和计算的资源有限[5]. 传感器节点感测的数据通过公共网络传输的,且传感器节点常常部署在无人看管甚至敌对环境中[6],这

使得WSNs容易受到攻击.因此,提供安全的身份认证与密钥协商协议以验证用户身份并加密通信内容对保障网络安全至关重要.

如图1所示,一个典型的WSNs多因素身份认证协议包含3类参与方:一个或多个网关,一组用户,以及大量的传感器节点.考虑到传感器节点的计算和存储资源受限,且WSNs通常应用在高安全需求的场景中,身份认证与密钥协商协议应该是轻量级的、能抵抗各类已知攻击、且具备用户匿名、前向安全等理想属性[6].通常来说,WSNs环境的身份认证流程有以下几步:(1)用户及传感器节点在网关注册,成为合法参与方.(2)当用户想访问某传感器节点的实时数据时,需先向本地网关发起访问请求,这一过程称为登录阶段.(3)若用户请求访问的传感器节点处于本地网关网络覆盖范围,则本地网关对用户完成认证后,向传感器节点传达用户请求,并与传感器节点进行双向认证;若用户请求访问的传感器节点处于外部网关网络覆盖范围,则本地网关在认证用户身份后,需向外部网关发起访问请求,并进行双向认证,然后外部网关向传感器节点传达用户请求.(4)本地网关或外部网关把传感器的响应转发给用户,用户验证传感器的响应后完成认证.认证结束后,用户与传感器节点之间会协商出一个会话密钥来保护后续通信.

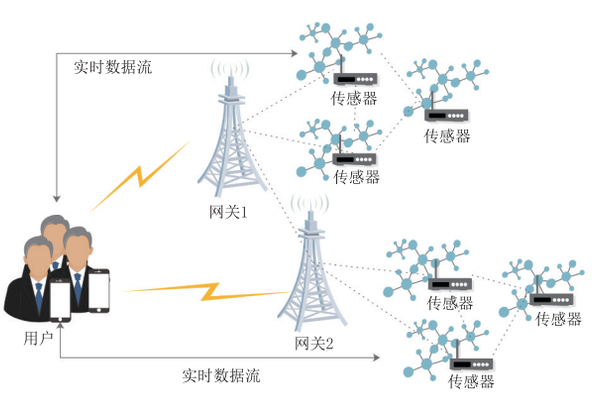

图1　面向多网关的无线传感器网络用户身份认证架构

在认证用户身份时,所依据的信息一般包含3类:用户所知道的信息,如口令;用户所拥有的东西,如智能卡;用户的生物特征,如指纹.在认证用户时,使用2种及以上信息的协议称为多因素认证协议.大部分面向多网关的WSNs用户身份认证协议利用网关之间共享的秘密参数来实现不同网关之间的认证,如Srinivas等协议[5],但也有少部分协议使用基站充当认证中心来实现认证,如Ali等协议[7].前者适用于具备海量网关和传感器节点的场景,更符合物联网的发展趋势.

1.1　相关工作

2009年,Das等[8]首次提出了一个高效的基于智能卡的口令身份认证协议,为用户访问传感器节点中的实时数据提供了基本保障.然而,Khan等[9]和Chen等[10]随后指出Das等[8]协议存在安全威胁,如无法抵抗离线字典猜测攻击、仿冒攻击、内部攻击等.同时,为改进Das等协议,Khan等[9]、Chen等[10]分别提出了新的认证协议,他们的协议实现了通信三方的双向认证,解决了Das等协议的一些问题,但依旧被Vaidya等[11]发现存在诸多安全漏洞,如易遭受节点捕获攻击、节点仿冒攻击、智能卡丢失攻击等.2014年,Turkanović等[12]设计了一个新型轻量级的双因素用户认证协议,企图克服之前协议中的安全漏洞,他们通过形式化分析、逻辑推理以及仿真工具证明了协议的安全性.

不幸的是,Amin等[13]在2016年表明他们的协议无法抵抗离线字典猜测攻击、用户仿冒攻击、传感器节点仿冒攻击.另外考虑到无限传感器网络技术在物联网中的应用,面向多网关的WSNs用户身份认证已然成为了新的研究难题与热点,于是Amin等[13]提出了一个面向多网关的用户身份认证协议.在该协议中,用户的身份认证存在2种场景:在场景1中,用户访问的目标节点在用户本地网关所在的覆盖范围内,只涉及3个参与方的相互认证;在场景2中,用户访问的目标节点不在本地网关网络所在的覆盖范围内,因此需要广播用户请求,先与外部网关完成认证,涉及4个参与方之间的相互认证.Wu等[14]以及Srinivas等[5]在指出Amin等[13]协议的安全威胁后,分别提出了改进协议.2018年,Ali等[7]提出了新型的面向多网关的用户认证协议.在该协议中,基站扮演认证中心的角色,统一管理用户与传感网络之间的认证,因而无论用户访问的是本地网关还是外部网关,其认证方式完全一样.

1.2　研究动机与贡献

尽管经过了10年发展,设计一个安全的WSNs多因素身份认证协议依旧面临巨大挑战[6].一方面,随着物联网的发展,无线传感网络技术的应用范围越来越广,无论是民用和军用还是环境和医疗监测,无线传感网络技术都能提供良好的信息处理和收集功能.一方面,这些系统通常处理敏感的应用数据,对协议的安全性有更高要求;另一方面,传感器节点受资源约束,对加密原语的计算成本要求很高.面

向多网关的WSNs身份认证协议涉及到更多通信方之间的交互,且需要完成不同的信任域之间的相互认证,因而面临着更大的挑战.此外,前向安全性能够保障系统被攻破后,不会泄漏之前的通信内容,在一些重要的工业物联网应用中是一个很重要的安全属性.但实际上,据我们所知,当前几个面向多网关的身份认证协议都无法实现前向安全性.总而言之,如何有效地完成对外部网关的认证,且抵抗各类攻击、提供良好的安全属性(如,前向安全性)是面向多网关的WSNs多因素用户身份认证的难题.本文通过对两个典型的多网关环境下用户认证协议的分析,指出此类协议存在的普遍问题,提出改进的多因素身份认证协议.本文的贡献可分为以下3个方面:

1) 指出Ali等的协议[7]易受到离线字典猜测攻击、节点仿冒攻击、内部攻击,且无法提供前向安全性和用户匿名;指出Srinivas等的协议[5]无法抵抗离线字典猜测攻击和内部攻击,没有实现用户匿名和前向安全;讨论了这些安全问题产生的根本原因及解决方法.

2) 设计了一个安全的基于椭圆曲线密码算法的多因素身份认证协议.协议通过网关之间共享的秘密参数来实现网关之间的认证.

3) 通过BAN逻辑分析及启发式分析证明了改进的协议能够实现双向认证、安全地建立会话密钥以及抵抗各类已知的攻击;与相关典型的协议的对比分析显示协议实现了更好的安全性.

1.3 组织结构

第2节介绍了攻击者模型及评价指标;第3节和第4节回顾并分析了Ali等的协议的安全问题;第5节和第6节指出了Srinivas等的协议的不足之处;第7节提出了改进的身份认证协议;第8节和第9节分析了协议的安全性;第10节从安全和性能两方面对比分析相关协议;最后,第11节小结全文.

2 攻击者模型及评价指标

基于文献[5-7,15,18],本节提出多网关无线传感器网络用户身份认证协议的攻击者模型及评价指标.文本用到的符号及其含义如表1所示.

表1 符号定义

符号	含义
GWN_k	第k个网关节点
U_i/U_i^k	第i个(位于GWN_k中)用户
SN_j/SN_j^k	第i个(位于GWN_k中)传感器节点
$PW_i/ID_i/ID_i^k$	用户U_i的口令和身份标识
Bio_i	用户U_i的生物特征
$X_{SN_j}^k$	传感器节点SN_j/SN_j^k的私钥
ID_{SN_j}/SID_j^k	传感器节点SN_j/SN_j^k的身份标识
X	基站的长期秘密私钥
X_{BS-GWN_k}	基站与网关GWN_k之间的秘密参数
X_{GWN}^k	网关GWN_k的长期秘密私钥
ID_{GWN}/GID_k	GWN_k的身份标识
S_{ran}	网关之间共享的密钥
$E(\cdot)/D(\cdot)$	加密函数/解密函数
$Gen(\cdot)/Rep(\cdot)$	生物特征提取/恢复函数
$H(\cdot)$	针对生物特征的哈希函数
$h(\cdot)$	哈希函数
$\oplus$	异或运算
$\|$	比特连接运算
$A\rightarrow B:M$	将消息M通过普通信道由A传送到B
$A\Rightarrow B:M$	将消息M通过安全信道由A传送到B

2.1 攻击者模型

通常来说面向多网关的WSNs多因素用户身份认证协议的攻击者具备如下能力:

C1. 攻击者能够完全控制公开信道,即能够任意窃听、拦截、修改或者阻断流经公开信道中的消息[5-7,18].

C2. 攻击者能够同时离线列举用户口令空间和身份标识空间中的所有元素,特别地,在评估协议抗攻击性强度时,攻击者可以得到用户的身份标识[6,15,18].

C3. 在n-因子协议中($n=2$或3),攻击者可以获得任意$n-1$个因子[18].

C4. 攻击者可以获取之前的会话密钥[6,15,18].

C5. 仅在评估前向安全性时,攻击者能够获得系统(通常是网关)的长期秘密私钥[6,15].

C6. 攻击者能够捕获有限数量的传感器节点,获取存储在节点中的数据[5-7].

C7. 攻击者可以是一个合法用户.评估用户注册阶段安全性时,攻击者可以是注册中心(基站/网关)管理员[6,18].

需注意,本文采用的攻击者模型,在不考虑评估协议的前向安全性时,假设网关和/或基站是可信的,攻击者不会仿冒其他网关、用户和传感器节点,且存储在网关和基站中的数据也是安全的.

2.2 评价指标

2018年,Wang等[6]在文献[17]的基础上,提出了适用于无线传感网络的评价指标.该标准是当前最先进的评价标准,本文将采用这一标准.该标准

包含11项评价指标,具体如下:

S1:无口令验证表.在网关和传感器上不应该存储用户口令相关的验证表.

S2:口令友好性.用户能够自主选择口令,并在本地修改口令.

S3:口令安全性.用户的口令不能被内部特权管理员(网关或者基站)获取或计算出来.

S4:抗智能卡丢失攻击.拥有受害者智能卡的攻击者无法利用智能卡中的信息来提高攻击优势.

S5: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.

S6:可修复性.支持智能卡撤销及动态节点添加.

S7:建立会话密钥.在认证完成后,传感器节点和用户之间要建立共享的会话密钥.

S8:无需时钟同步.协议不受时钟同步和时延的影响,即服务器和客户端不需要将它们的时钟与所有输入设备同步.

S9:双向认证.通信参与方之间要相互认证.

S10:用户匿名.协议应保护用户身份标识,且实现身份标识的不可追跟踪性.

S11:前向安全性.攻击者即使获得了长期秘密私钥或者完全攻破了某一通信方,也无法计算之前的会话密钥.前向安全性可视为系统安全的最后一道防线,能够极大程度地降低系统被攻破后的损失,因而一直被学术及工业界视为重要的安全属性.最近颁布的TLS 1.3标准①和WPA3标准②也都要求用户认证协议能实现前向安全性.

3　Ali等人的协议回顾

本节回顾Ali等[7]在2018年提出的适用于农业监测的无线传感网络安全认证与密钥协商协议.该协议包含6个阶段,但限于篇幅,本节省略与文本关联不大的口令更新和传感器节点动态增加阶段.

3.1　系统初始化

系统管理者为传感器节点SN_j选取唯一身份标识ID_{SN_j},为网关节点GWN_k选取身份标识ID_{GWN_k},计算$X_{SN_j}=h(ID_{SN_j}\|X)$,将$\{X_{SN_j},ID_{SN_j}\}$存入SN_j.

3.2　用户注册阶段

R1. 用户U_i选取身份标识ID_i和口令PW_i,并输入生物特征Bio_i,计算$Gen(Bio_i)=(X_F,P_F)$,$RPW_i=h(PW_i\|X_F)$.

R2. $U_i\Rightarrow BS:\{ID_i,RPW_i\}$.

R3. BS计算$A_i=h(ID_i\|X)$,$B_i=A_i\oplus h(RPW_i\|ID_i)$,$C_i=A_i\oplus h(B_i\|X)$,$D_i=h(A_i\|RPW_i\|ID_i)$,BS将$\{B_i,C_i,D_i,h(\cdot)\}$写入智能卡.

R4. $BS\Rightarrow U_i$:智能卡.

R5. U_i将P_F写入智能卡.

3.3　登录阶段

L1. 用户U_i将智能卡插入读卡器,输入ID_i、PW_i和Bio_i,然后智能卡计算$Rep(Bio_i,P_F)=X_F^*$,$RPW_i^*=h(PW_i\|X_F^*)$,　$A_i^*=B_i\oplus h(RPW_i^*\|ID_i)$,$D_i^*=h(A_i^*\|RPW_i^*\|ID_i)$,$[h(B_i\|X)]^*=C_i\oplus A_i^*$,并比较$D_i^*$是否等于$D_i$.如果相等,执行下一步骤,否则,终止会话.

L2. U_i生成随机数R_U,计算$DID_i=ID_i\oplus h(B_i\|X)$,$M_1=E_{A_i}(R_U\|ID_{SN_j}\|ID_{GWN_j}\|T_1)$,$M_2=h(R_U\|ID_i\|T_1\|h(B_i\|X))$.

L3. $U_i\rightarrow BS:\{B_i,DID_i,M_1,M_2\}$.

3.4　认证与会话密钥协商阶段

V1. BS计算$ID_i^*=DID_i\oplus h(B_i\|X)$,$(R_U^*\|ID_{SN_j}^*\|ID_{GWN_j}^*\|T_1)=D_{A_i}(M_1)$,并判断是否满足$T_2-T_1\leqslant\Delta T$,其中$T_2$是当前时间戳,$\Delta T$是消息的最大时间传输延迟.计算$M_2^*=h(R_U^*\|ID_i^*\|T_1\|h(B_i\|X))$,比较$M_2^*$是否等于$M_2$,如果相等,$BS$相信用户是合法的,执行下一步骤;否则,终止会话.

V2. 基站BS首先生成一个随机数R_{BS},计算$M_3=E_{h(X_{BS-GWN_j})}(ID_i\|X_{SN_j}\|ID_{SN_j}\|R_U\|R_{BS}\|T_3)$　$M_5=h(M_2\|ID_i\|T_3\|R_{BS}\|R_U)$.

V3. $BS\rightarrow GWN_j:\{M_3,M_2,M_5\}$.

V4. GWN_k计算$(ID_i\|X_{SN_j}\|ID_{SN_j}\|R_U\|R_{BS}\|T_3)=D_{h(X_{BS-GWN_k})}(M_3)$,$M_5^*=h(M_2\|ID_i\|T_3\|R_{BS}\|R_U)$,检查$T_3$,并比较$M_5^*$是否等于$M_5$.如果同时满足,执行下一步骤;否则,终止会话.

V5. GWN_k生成随机数R_{GWN_j},计算$M_6=E_{X_{SN_j}}(R_{BS}\|\ T_5\|R_U\|R_{GWN_j}\|ID_i)$,$M_7=h(M_2\|X_{SN_j}\|R_{GWN_j}\|ID_i\|R_U)$.

① The Transport Layer Security (TLS) Protocol Version 1.3, https://www.rfc-editor.org/info/rfc8446, 2018

② Wi-Fi security is starting to get its biggest upgrade in over a decade. https://www.theeverge.com/circuitbreaker/2018/26/17501594/wpa3-wifi-security-certification, 2018

V6. $GWN_k \rightarrow SN_j$:{M_2, M_6, M_7}.

V7. SN_j 计算 $(R_{BS}\|T_5\|R_U\|R_{GWN_j}\|ID_i)=D_{X_{SN_j}}(M_6)$, $M_7^*=h(M_2\|X_{SN_j}\|R_{GWN_j}\|ID_i\|R_U)$, 检查 T_5 是否有效,并比较 M_7^* 是否等于 M_7. 如果同时满足,执行下一步骤,否则,终止会话.

V8. SN_j生成随机数R_{SN_j},计算$M_8=R_{SN_j}\oplus h(X_{SN_j}\|R_{GWN_j})$, $SK=h(R_{GWN_j}\|R_U\|R_{SN_j}\|X_{SN_j}\|M_2)$, $M_9=h(SK\|ID_i)$.

V9. $SN_j \rightarrow GWN_k$:{M_8, M_9, T_7}.

V10. GWN_k检查,计算$R_{SN_j}^*=M_8\oplus h(X_{SN_j}\|R_{GWN_j})$, $SK^*=h(R_{GWN_j}\|R_U\|R_{SN_j}^*\|X_{SN_j}\|M_2)$, $M_9^*=h(SK^*\|ID_i)$, 并比较 M_9^* 是否等于 M_9. 如相等,计算 $M_{10}=E_{h(R_U\|ID_i)}(X_{SN_j}\|T_9\|R_{GWN_j}\|R_{SN_j}\|M_2)$;否则,终止会话.

V11. $GWN_k \rightarrow U_i$:{M_9, M_{10}}.

V12. U_i 首先计算 $(X_{SN_j}\|T_9\|R_{GWN_j}\|R_{SN_j}\|M_2)=D_{h(R_U\|ID_i)}(M_{10})$, 检查 T_9 是否有效. 如果有效,计算 $SK^*=h(R_{GWN_j}\|R_U\|R_{SN_j}\|X_{SN_j}\|M_2)$, $M_9^*=h(SK^*\|ID_i)$, 并比较 M_9^* 是否等于 M_9. 如果相等,则 U_i 和 SN_j 完成相互认证.

4 Ali等协议安全性分析

本节分析Ali等协议[7]的安全性. 分析结果表明该协议无法抗离线字典猜测攻击、内部攻击和用户仿冒攻击,无法实现用户匿名性和前向安全性.

4.1 离线字典猜测攻击Ⅰ

在非抗窜扰智能卡的假设下,攻击者 $\mathcal{A}$ 可通过恶意扫描器获得用户生物特征 Bio_i,以及侧信道技术获得智能卡内信息{$B_i, C_i, D_i, h(\cdot), P_F, Gen(\cdot)$},发起如下离线字典猜测攻击:

步骤1:$\mathcal{A}$从用户身份空间 $\mathcal{D}_{id}$ 和口令空间 $\mathcal{D}_{pw}$ 猜测(ID_i^*, PW_i^*);

步骤2:$\mathcal{A}$ 计算 $Rep(Bio_i, P_F)=X_F^*$, $RPW_i^*=h(PW_i\|X_F^*)$, $A_i^*=B_i\oplus h(RPW_i^*\|ID_i)$, $D_i^*=h(A_i^*\|RPW_i^*\|ID_i)$;

步骤3:验证$D_i^*=D_i$是否成立. 如果成立,则猜测正确,否则转步骤1.

实际上,Wang等[19]在2015年指出,该攻击与本地修改口令这一功能要求存在矛盾:一个协议如果要实现本地改口令,则必须在智能卡中存储对应的验证参数,而这个验证参数恰好可以被攻击者用来验证所猜测口令的正误. 为解决这个矛盾,2016年,Wang等[17]引入fuzzy-verifier技术,结合honey words,有效地解决了这个问题,使得用户可以安全地在本地修改口令.

以Ali等协议[7]为例,依据Wang等[17]方法,需将 D_i 修改为 $D_i=h(A_i^*\|RPW_i^*\|ID_i^*) \bmod n_0$, 其中 $n_0\in[2^4, 2^8]$,并在BS中存储honey-list来记录用户登录失败的次数. 这样一来,即使攻击者成功地按照上述步骤找到了一对满足条件的(ID_i^*, PW_i^*),但考虑到符合上述等式的口令和身份标识有 $\frac{|\mathcal{D}_{id}*\mathcal{D}_{pw}|}{n_0}\approx 2^{32}$个,因此攻击者只能通过线上登录来确认,但由于honey-list会记录用户登录失败的次数,一旦超过一定的阈值(比如10),就会冻结智能卡,从而阻止该攻击.

4.2 离线字典猜测攻击Ⅱ

除利用智能卡中的验证因子发起离线字典猜测攻击,攻击者还能够借助信道中的验证因子执行类似攻击. 攻击者一旦拿到用户 U_i 智能卡中的数据{$B_i, C_i, D_i, h(\cdot), P_F, Gen(\cdot)$}和生物特征 Bio_i,并且窃听到 U_i 发送给基站的访问请求,则可利用用户与基站之间的验证因子执行如下离线字典猜测攻击.

步骤1:A 从用户身份空间 D_{id} 和口令空间 D_{pw} 猜测(ID_i^*, PW_i^*);

步骤2:A 计算 $Rep(Bio_i, P_F)=X_F^*$, $RPW_i^*=h(PW_i\|X_F^*)$, $A_i^*=B_i\oplus h(RPW_i^*\|ID_i)$, $h(B_i\|X)=C_i\oplus A_i^*$,用 A_i^* 解密 M_1,得到 $R_U\|ID_{SN_j}\|ID_{GWN_j}\|T_1$,计算 $M_2^*=h(R_U\|ID_i\|T_1\|h(B_i\|X))$;

步骤3:验证 $M_2^*=M_2$ 是否成立. 如果成立,则猜测正确,否则,转步骤1.

该攻击发生的主要原因在于,用户发送给基站进行身份验证的验证因子 M_2 能够通过生物特征、智能卡中的数据和口令推导出来,因此攻击者可以用该验证因子 M_2 来检测猜测的口令是否正确. 为抵抗该攻击,公钥算法是必要的[19]. 为方便解释不妨假设采用椭圆曲线公钥算法,$E(q)$为椭圆曲线E的一个子集,P为$E(q)$上的某个点,X为基站BS的私钥,$Y=X\cdot P$为对应的公钥,则如果用户计算 $K=r_i\cdot Y$, $K_0=r_i\cdot P$, $M_2=h(R_U\|ID_i\|T_1\|h(B_i\|X\|K\|K_0)$,并把 M_2 和 K_0 发送给 BS,则 BS 可以用私钥 X 计算出 M_2,但攻击者无法用猜测的口令和身份标识表示出 M_2,从而无法执行上述攻击.

4.3 前向安全性问题

假设攻击者 $\mathcal{A}$ 获取了基站 BS 的长期秘密私钥

X,并截获U_i发往BS的消息$\{B_i, DID_i, M_1, M_2\}$以及GWN_k发往U_i的消息$\{M_9, M_{10}\}$,则可获取U_i和SN_j的会话密钥,具体流程如下:

步骤1:攻击者A计算$ID_i = DID_i \oplus h(B_i \| X)$,$A_i = h(ID_i \| X)$,$(R_U \| ID_{SN_j} \| ID_{GWN_j} \| T_1) = D_{A_i}(M_1)$,$(X_{SN_j} \| T_9 \| R_{GWN_j} \| R_{SN_j} \| M_2) = D_{h(R_U \| ID_i)}(M_{10})$.

步骤2:A计算会话密钥$SK = h(R_{GWN_j} \| R_U \| R_{SN_j} \| X_{SN_j} \| M_2)$.

通过上述攻击,攻击者$\mathcal{A}$可获得U_i与传感器节点之间的会话密钥.由于U_i的长期秘密值A_i与基站BS的长期秘密私钥唯一相关,一旦密钥X泄漏,攻击者便可获得所有用户与所访问传感器节点的会话密钥,威胁整个系统安全性.

面向传感器网络的用户身份认证协议普通无法实现前向安全,主要原因在于,为了能够保障协议在资源受限的传感器节点上的运行效率,认证协议多数仅使用哈希函数等对称密码算法.然而,Ma等[20]指出,为实现前向安全性,首先需要采用公钥算法,其次在服务器端(即传感器节点)必须执行至少2次模幂或者椭圆曲线点乘运算.随着攻击技术的不断发展,服务器(网关/基站)被攻破的案例层出不穷[18,21],前向安全性作为保护系统安全的一个重要属性,应当予以重视,适当牺牲性能以实现前向安全性可取.

4.4　内部攻击

2019年,Li等[18]首次系统地分析了长期被忽视的内部攻击,并提出了相应的解决方法.在Ali等人协议中,攻击者$\mathcal{A}$能够在注册阶段获取用户发送的$RPW_i = h(PW_i \| X_F)$,若$\mathcal{A}$又得到了U_i的生物特征Bio_i,则可通过如下步骤成功猜测出U_i的口令:

步骤1:A从用户身份空间D_{id}和口令空间D_{pw}猜测(ID_i^*, PW_i^*);

步骤2:A计算$Rep(Bio_i, P_F) = X_F^*$,$RPW_i^* = h(PW_i^* \| X_F^*)$;

步骤3:验证$RPW_i^* = RPW_i$是否成立.如果成立,则猜测正确,否则转步骤1.

根据Li等[18]提出的解决协议,其核心在于,首先用户向注册中心(基站或者网关)发送用随机数a保护的PW_i,如$RPW_i = h(PW_i \| a)$;其次,在拿到智能卡后,协议需更新已使用过的随机数a.如此,攻击者即使获取了用户智能卡中的信息或生物特征以及登录请求,但因无法得到随机数a来构造RPW_i,依旧无法执行上面的攻击.

4.5　传感器节点仿冒攻击

假设攻击者$\mathcal{A}$注册成为了一个合法的用户U_i,并向任意一个传感器节点SN_j发起了访问请求,则攻击者$\mathcal{A}(U_i)$可计算$h(R_U \| ID_i)$来解密M_{10}得到传感器节点的私钥X_{SN_j}.一旦得到了SN_j的私钥,则攻击者能够向所有参与者仿冒SN_j.该攻击是在协议设计时未充分考虑攻击者能力引发的.

4.6　匿名性失效

随着用户隐私保护意识的提高,保障用户匿名已经成为身份认证协议的基本要求之一.匿名性有两个层次的含义:(1)基本层次要求攻击者无法获知用户的真实身份标识,即用户ID保护;(2)高级层次要求攻击者无法分辨出两个会话是否由同一用户参与,即用户不可追踪性.Ali等人协议未实现用户行为的不可追踪性.假设攻击者$\mathcal{A}$在信道中窃听得到了用户发给基站的信息,则$\mathcal{A}$可以通过固定的DID_i从众多会话中识别出由同一个用户发送的消息,进而可以分析出用户的行为特点或兴趣爱好等,以达到某些商业目的,如精准推销或者广告[19].

5　Srinivas等人的协议回顾

2017年,Srinivas等[5]提出了一个多网关无线传感网络用户认证协议,该协议包含两个应用场景:在场景1中,用户访问的目标传感器节点在本地网关覆盖范围内,只涉及3个参与方之间的相互认证;在场景2中,用户访问的目标传感器不在本地网关覆盖范围内,需要先认证外部网关的身份,涉及到4个参与方之间的认证.在Srinivas等人协议中,场景2中面临的安全威胁与场景1类似,故本文以场景1为例来分析Srinivas等协议.

5.1　系统初始化

系统管理者SA为传感器节点SN_j选取唯一身份标识ID_{SN_j},计算$X_{SN_j} = h(ID_{SN_j} \oplus S_{ran})$,其中$S_{ran}$是网关节点$HGWN$的一个随机秘密值,然后将$\{X_{SN_j}, ID_{SN_j}\}$写入$SN_j$,把$SN_j$部署在目标区域.

5.2　传感器注册阶段

R1. SN_j计算$M_j = h(ID_{SN_j} \| X_{SN_j} \| T_r)$戳.

R2. $SN_j \rightarrow HGWN$:$\{ID_{SN_j}, T_r, M_j\}$.

R3. $HGWN$计算$X_{SN_j} = h(ID_{SN_j} \oplus S_{ran})$,然后$h(D_{SN_j} \| X_{SN_j} \| T_r)$是否等于接收到的$M_j$.若相等,$HGWN$将$\{ID_{SN_j}, T_r\}$存入数据库.

R4. SN_j保存T_r.

5.3 用户注册阶段

R1. 用户U_i选取ID_i和PW_i,生成随机数u,计算$DID_i=h(ID_i\|u)$,$RPW_i=h(PW_i\|u\|ID_i)$.

R2. $U_i\Rightarrow HGWN$:$\{DID_i, RPW_i\}$.

R3. $HGWN$检查DID_i是否已注册.若未注册,选取随机数TID_i,计算$K_i=h(DID_i\|TID_i\|X_{GWN}^H)$,$Y_i=K_i\oplus RPW_i$,其中$X_{GWN}^H$是$HGWN$的密钥.$HGWN$在数据库中存储$\{TID_i, DID_j\}$,将$\{Y_i, TID_i, h(\cdot)\}$写入智能卡中.

R4. $HGWN\Rightarrow U_i$: 智能卡.

R5. U_i输入生物特征Bio_i,计算$C_i=u\oplus H(Bio_i)$,$V_i=h(ID_i\oplus PW_i\oplus u)$,并将$C_i$和$V_i$写入智能卡.

5.4 登录阶段

L1. U_i输入ID_i,PW_i和Bio_i,计算$u=C_i\oplus h(Bio_i)$,比较计算$h(ID_i\oplus PW_i\oplus u)$是否等于智能卡中的$V_i$.如相等,计算$K_i=Y_i\oplus h(PW_i\|u\|ID_i)$.

L2. U_i向$HGWN$查询欲访问传感器节点的ID_{SN_j}.

L3. 智能卡选取随机数r_i,计算$DID_i=h(ID_i\|u)$,$D_1=h(K_i\|DID_i\|ID_{SN_j})\oplus r_i$,$D_2=h(DID_i\|r_i\|\ TID_i\|K_i\|T_1\|ID_{SN_j})$,其中$T_1$是当前时间戳.

L4. $U_i\rightarrow HGWN$:$\{TID_i, ID_{SN_j}, D_1, D_2, T_1\}$.

5.5 认证与密钥协商阶段

V1. $HGWN$检查用户要访问的传感器节点身份标识ID_{SN_j}是否在数据库中.如存在,检查T_1.提取DID_i,计算$K_i'=h(DID_i\|TID_i\|X_{GWN}^H)$,$r_i=D_1\oplus h(K_i'\|DID_i\|ID_{SN_j})$,$D_2'=h(DID_i\|r_i\|TID_i\|K_i'\|T_1\|ID_{SN_j})$.比较$D_2'$与$D_2$是否相等.如相等,$HGWN$成功认证$U_i$;否则,终止会话.

V2. $HGWN$生成随机数r_h,$X_{SN_j}=h(ID_{SN_j}\oplus S_{ran})$,$D_3=h(X_{SN_j}\|T_2\|T_r\|ID_{SN_j}\|TID_i)\oplus r_h$,$D_4=r_i\oplus h(X_{SN_j}\|TID_i\|r_h\|T_2)$,$D_5=DID_i\oplus h(X_{SN_j}\|r_i\|\ \ r_h\|T_2)$,$D_6=h(ID_{SN_j}\|r_i\|DID_i\|T_r\|X_{SN_j}\|\ r_h\|T_2)$.

V3. $HGWN\rightarrow SN_j$:$\{TID_i, D_3, D_4, D_5, D_6, T_2\}$.

V4. SN_j检查T_2,计算$r_h'=h(X_{SN_j}\|T_2\|T_r\|ID_{SN_j}\|TID_i)\oplus D_3$,$r_i'=D_4\oplus h(X_{SN_j}\|TID_i\|r_h'\|T_2)$,$DID_i'=D_5\oplus h(X_{SN_j}\|r_i'\|r_h'\|T_2)$,$D_6'=h(ID_{SN_j}\|r_i'\ \ \|DID_i'\|T_r\|X_{SN_j}\|r_h'\|T_2)$,比较$D_6'$与$D_6$是否相等.如相等,执行下一步骤;否则,终止会话.

V5. SN_j生成随机数r_j,计算$D_7=r_j\oplus h(X_{SN_j}\|r_h'\|T_3)$,$D_8=h(X_{SN_j}\|r_j\|T_2\|r_h'\|TID_i\|r_i'\|T_3\|T_r)$以及会话密钥$SK=h(DID_i\|r_i'\|r_j\|r_h'\|ID_{SN_j})$.

V6. $SN_j\rightarrow HGWN$:$\{D_7, D_8, T_3\}$.

V7. $HGWN$检查T_3,计算$r_j'=D_7\oplus h(X_{SN_j}\|r_h\|T_3)$,$D_8'=h(X_{SN_j}\|r_j'\|T_2\|r_h\|TID_i\|r_i\|T_3\|T_r)$,比较$D_8'$与$D_8$是否相等.如果相等,$HGWN$计算$D_9=r_h\oplus h(K_i\|DID_i\|r_i)$,$D_{10}=r_j\oplus h(K_i\|r_h\|\ \ DID_i\|r_i)$,$D_{11}=h(K_i\|DID_i\|r_j'\|T_1\|r_h\|T_4\|r_i)$,以及会话密钥$SK=h(DID_i\|r_i\|r_j'\|r_h\|ID_{SN_j})$

V8. $HGWN\rightarrow U_i$:$\{D_9, D_{10}, D_{11}, T_4\}$

V9. U_i接收到来自$HGWN$的消息后,首先检查T_4.如有效,U_i计算$r_h=D_9\oplus h(K_i\|DID_i\|r_i)$,$r_j=D_{10}\oplus h(K_i\|r_h\|DID_i\|r_i)$,$D_{11}'=h(K_i\|DID_i\|r_j\|T_1\|r_h\|T_4\|r_i)$比较$D_{11}'$与$D_{11}$是否相等.如果相等,则计算$SK=h(DID_i\|r_i\|r_j\|r_h\|ID_{SN_j})$.

6 Srinivas等协议安全性分析

本节对Srinivas等协议[5]进行分析,指出该协议存在的安全问题,例如,无法抵抗离线字典猜测攻击和内部攻击,无法实现前向安全和用户匿名.

6.1 离线字典猜测攻击I

假设攻击者$\mathcal{A}$通过侧信道攻击技术获得智能卡内敏感信息$\{Y_i, TID_i, h(\cdot), C_i, V_i\}$,并通过恶意扫描器获得用户生物信息$Bio_i$,则可发起口令猜测攻击:

步骤1:A从用户身份空间D_{id}和口令空间D_{pw}猜测(ID_i^*, PW_i^*);

步骤2:计算$u=C_i\oplus h(B_i)$,$V_i^*=h(ID_i^*\oplus PW_i^*\oplus u)$,其中$C_i$从智能卡中获得;

步骤3:验证$V_i^*=V_i$是否成立.如果成立,则(ID_i^*, PW_i^*)猜测正确,否则转步骤1.

该攻击与4.1节描述的攻击一致,本质上是用户本地改口令与抗离线字典猜测攻击之间的矛盾.同样的,采用fuzzy-verifier和honeywords[17]能够很好地解决此类攻击.

6.2 离线字典猜测攻击II

假设攻击者获得智能卡内敏感信息$\{Y_i, TID_i, h(\cdot), C_i, V_i\}$,和生物信息$Bio_i$,且得到了$U_i$发给网关$HGWN$的消息$\{TID_i, ID_{SN_j}, D_1, D_2, T_1\}$,则可以发起下面离线字典猜测攻击:

步骤1:A从用户身份空间D_{id}和口令空间D_{pw}猜测(ID_i^*, PW_i^*);

步骤2:A计算$u=C_i\oplus h(B_i)$, $K_i^*=Y_i\oplus h(PW_i^*\|u\|ID_i)$, $DID_i^*=h(ID_i^*\|u)$, $r_i^*=D_1\oplus h(K_i^*\|DID_i^*\|ID_{SN_j})$, $D_2^*=h(DID_i^*\|r_i^*\|TID_i\|K_i^*\|T_1\|ID_{SN_j})$;

步骤3:验证$D_2^*=D_2$是否成立.

如4.2所述,公钥算法是应对此类攻击的重要技术,仅采用哈希函数这一类对称密码算法无法抵抗此类攻击. 此外,攻击者还能够以场景1中的D_{11},场景2中的L_3和L_4为验证值完成该攻击.

6.3　前向安全性问题

假设攻击者$\mathcal{A}$获取了$HGWN$的秘密值S_{ran},并截获$HGWN$发往SN_j的消息$\{TID_i, D_3, D_4, D_5, D_6, T_2\}$及$SN_j$回送$HGWN$的消息$\{D_7, D_8, T_3\}$,则可获取$U_i$和$SN_j$的会话密钥,具体流程如下:

步骤1. A计算$X_{SN_j}=h(ID_{SN_j}\oplus S_{ran})$, $r_h=h(X_{SN_j}\|T_2\|T_r\|ID_{SN_j}\|TID_i)\oplus D_3$, $r_i=D_4\oplus h(X_{SN_j}\|TID_i\|r_h\|T_2)$;

步骤2. A计算$r_j=D_7\oplus h(X_{SN_j}\|r_h\|T_3)$,进一步得到会话密钥$SK=h(DID_i\|r_i\|r_j\|r_h\|ID_{SN_j})$.

6.4　内部攻击

Srinivas等协议[5]也无法抵抗内部攻击. 假设$\mathcal{A}$在注册阶段得到了$RPW_i=h(PW_i\|u\|ID_i)$,又获得了Bio_i以及智能卡中的C_i,则可猜测出U_i的口令:

步骤1:A从用户身份空间D_{id}和口令空间D_{pw}猜测(ID_i^*, PW_i^*);

步骤2:A计算$u=C_i\oplus h(Bio_i)$,以及$RPW_i^*=h(PW_i^*\|u\|ID_i)$;

步骤3:验证$RPW_i^*=RPW_i$是否成立. 如果成立,则猜测正确,否则转步骤1.

6.5　匿名性失效

尽管Srinivas等协议尽管实现了基本层次的匿名性,即用户ID保护,攻击者仍可追踪用户行为,对用户的隐私构成威胁. 用户U_i向网关节点$HGWN$发送登录请求消息$\{TID_i, ID_{SN_j}, D_1, D_2, T_1\}$,$HGWN$收到$U_i$的登录请求后,向传感器节点发送消息$\{TID_i, D_3, D_4, D_5, D_6, T_2\}$. 其中$TID_i$是$HGWN$选取的用于恢复用户匿名身份$DID_i$的一个随机数. TID_i长期保存在$HGWN$数据库及用户智能卡中,与用户U_i直接相关且固定不变. 因而$\mathcal{A}$可通过跟踪固定参数TID_i获得用户U_i的访问行为.

7　提出的新协议

对Ali等协议[7]和Srinivas等协议[5]的分析可发现,离线字典猜测攻击、内部攻击、前向安全性和用户匿名性失效问题是身份认证协议面临的主要安全漏洞. 本节提出一个改进的面向多网关的无线传感器网络身份认证协议,克服了这些安全漏洞.

7.1　设计思想

根据前面的分析,改进的协议采用了基于椭圆曲线的公钥算法,整合了fuzzy-verifier和honeywords来抵抗两类离线字典猜测攻击,并保障了匿名性;在传感器节点上执行了2次椭圆曲线点乘操作以实现前向安全性;采用Li等[18]推荐方法来抵抗内部攻击. 具体来说,针对第2.2节中的11个评价指标,本文提出的解决方案如表2所示.

此外,为顺应物联网环境下大规模传感器的节点应用的普及发展,本协议采用Srinivas等协议[5]的方法来实现不同网关之间的相互认证,即不需要认证中心来统一认证不同的网关. 特别地,在秘密参数的分配方面,本协议保证不同网关之间只共享一个秘密参数,任何网关都只能获取自身网络覆盖范围内的用户和传感器节点的秘密参数,这样能够极大地提高系统抵抗攻击的能力. 在Srinivas等协议[5]中,网关GWN_k可以计算非区域范围内的传感器节点$SN_j^m$$(m\neq k)$的私钥$h(ID_{SN_j}\|S_{ran})$($S_{ran}$为所有网关共享的参数),这是一种非常不安全的做法. 为减轻这一安全隐患,本协议让每个网关都拥有各自独立的长期秘密私钥X_{GWN}^k,各区域内的用户及传感器节点都用本区域内的长期秘密私钥X_{GWN}^k来计算相关参数,网关之间通过共享的S_{ran}认证.

如图2和图3,本协议一共包含两个认证场景,7个阶段:系统初始化、用户注册、用户登录、认证、口令更新、重注册及动态节点增加.

7.2　系统初始化

系统管理员选择椭圆曲线E的一个子集$E(q)$,为网关GWN_k在$E(q)$上的选取某个点P_k以及私钥X_{GWN}^k,计算其公钥$Y=X_{GWN}^k\cdot P_k$,并选取唯一的身份标识GID_k,最后将$\{X_{GWN}^k, GID_k\}$存入网关GWN_k中. 此外,系统管理员还需要为每个传感器节点SN_j^k选取唯一的身份标识SID_j^k,将其存储在传感器节点SN_j^k中,并把传感器节点部署在目标区域.

表2 针对11个指标的设计思想

指标	处理方法
S1	在网关仅存储用户的身份标识以及注册的时间，在传感器节点上不存储用户相关的任何参数.
S2	在注册阶段用户自主选择口令在网关进行注册；在智能卡中存储模糊验证因子，使用户可在本地更新口令.
S3	采用Li等人[18]建议，在注册阶段选择一个随机数a'来保护用户口令，并在得到网关的响应后，更新该随机数a'为a，并重新计算与a'相关的所有参数. 这样一来，即使拥有特权的网关管理员也无法得到用户的口令.
S4	主要说明对两类离线口令字典猜测攻击的处理方法：智能卡中存储模糊验证因子A_i，网关存储honey-list来记录用户失败次数，根据4.1节的分析，攻击者无法执行离线口令猜测攻击I；令网关与用户之间的认证因子M_2包含采用公钥技术传递的秘密参数K_2，根据4.2节的分析，攻击者无法执行离线口令猜测攻击II.
S5	随机数机制可以抵抗重放攻击、公钥密码技术为协议的安全性提供了基本的保障.
S6	协议提供了智能卡撤销及动态节点添加阶段.
S7	认证完成后，传感器节点和用户之间建立了共享的会话密钥SK.
S8	网关、传感器节点以及用户之间不需要将它们的时钟与所有输入设备同步.
S9	协议的通信架构保证了网关、传感器节点以及用户之间可以进行相互认证.
S10	采用公钥技术生成的秘密参数K_2来保护用户身份标识，且每轮会话中的K_2是不同的. 具体来说，用户身份标识ID_i^k不直接传递给网关，而以$M_2=ID_i^k\oplus h(K_1\|K_2)$的形式发送给网关，由于$K_2$是用公钥技术传递的参数，除用户外，只有拥有私钥的网关才能用信道中的K_1计算出K_2，因而攻击者无法计算ID_i^k；另一方面，K_1与K_2由随机数计算，其值随着每轮用户选择的不同的随机数而变化，因而攻击者无法追踪ID_i^k.
S11	采用Ma等人[20]建议，1)使用公钥技术来生成会话密钥中的参数，2)在传感器端执行2次椭圆曲线点乘.

7.3 传感器注册阶段

R1. $SN_j^k\Rightarrow GWN_k$：注册请求.

R2. $GWN_k\Rightarrow SN_j^k$：$\{X_{SN_j}^k=h(SID_j^k\|X_{GWN}^k)\}$.

R3. SN_j^k存储$X_{SN_j}^k$.

7.4 用户注册阶段

R1. ${U_i}^k\Rightarrow GWN_k$：$\{ID_i^k, RPW_i'\}$. 用户${U_i}^k$输入身份信息(ID_i^k, PW_i^k, Bio_i)，选择随机数a'，计算：$Gen(Bio_i)=(\delta_i,\tau_i)$，$RPW_i'=h(PW_i\|\delta_i\|a')$.

R2. GWN_k首先检查ID_i^k是否在数据库中. 若存在，则让用户选择一个新的ID_i^k；否则，计算$X_{U_i}^k=h(ID_i^k\|X_{GWN}^k\|T_{rg_i})$，$B_i'=h(RPW_i'\|ID_i^k)\oplus X_{U_i}^k$，并将$\{ID_i^k, T_{rg_i}, \text{honey-list}=0\}$存储在数据库中. 其中，$T_{rg_i}$为当前的时间戳.

R3. $GWN_k\Rightarrow {U_i}^k$：智能卡$\{B_i', Y_k, P_k\}$.

R4. 智能卡选择一个随机数a，计算$X_{U_i}^k=B_i'\oplus h(RPW_i'\|ID_i^k)$，$A_i=h(ID_i^k\|PW_i^k\|\delta_i\|X_{U_i}^k)\bmod n_0$，$RPW_i=h(PW_i^k\|\delta_i\|a)$，$B_i=h(RPW_i\|ID_i^k)\oplus X_{U_i}^k$，$n_0$为$[2^4, 2^8]$为间的整数，然后存储$\{A_i, B_i, a, \tau_i, Y_k, P_k\}$.

7.5 用户登录阶段

L1. 用户输入$\{ID_i^k, PW_i^k, Bio_i\}$，智能卡计算$\delta_i^*=Rep(Bio_i,\tau_i)$，$RPW_i^*=h(PW_i^k\|\delta_i^*\|a)$，$X_{U_i}^k=B_i\oplus h(RPW_i^*\|ID_i^k)$，$A_i^*=h(ID_i^k\|PW_i^k\|\delta_i^*\|X_{U_i}^k)\bmod n_0$. 比较$A_i^*$与$A_i$的大小，若相等，则继续后面的计算；否则，终止该会话.

L2. 智能卡选择一个随机数r_i，计算$K_1=r_i\cdot P_k$，$K_2=r_i\cdot Y_k$，$M_1=h(X_{U_i}^k\|ID_i^k\|K_1\|K_2)$，$M_2=ID_i^k\oplus h(K_1\|K_2)$，$EID_j=SID_j^k\oplus h(ID_i^k\|K_2)$. 注意，此处传感器节点身份标识$SID_j^k$，是用户向$GWN_k$询问所得.

L3. ${U_i}^k\rightarrow GWN_k$：$MSG_1=\{K_1, M_1, M_2, EID_j\}$.

7.6 场景1的认证与密钥协商阶段

V1. 收到${U_i}^k$的请求，GWN_k计算$K_2'=X_{GWN}^k\cdot K_1$，$ID_i^{k'}=M_2\oplus h(K_1\|K_2)$，$X_{U_i}^{k'}=h(ID_i^{k'}\|X_{GWN}^k\|T_{rg_i})$，$M_1'=h(X_{U_i}^{k'}\|ID_i^{k'}\|K_1\|K_2)$. 比较$M_1'$与$M_1$的大小，若相等，则继续后面的计算；否则，终止该会话，并且令honey-list=honey-list+1，且一旦honey-list的值超过10，则冻结该用户的账户，直至${U_i}^k$重注册.

V2. GWN_k选择r_g^k，$SID_j^{k'}=EID_j\oplus h(ID_i^{k'}\|K_2)$，$X_{SN_j}^{k'}=h(SID_j^{k'}\|X_{GWN}^k)$，$M_3=h(SID_j^{k'}\|K_1\|X_{SN_j}^{k'}\|r_g^k)$，$M_4=r_g^k\oplus h(X_{SN_j}^{k'}\|SID_j^{k'}\|K_1')$.

V3. $GWN_k\rightarrow SN_j^k$：$MSG_2=\{K_1, M_3, M_4\}$.

V4. SN_j^k计算$r_g^{k'}=M_4\oplus h(X_{SN_j}^k\|SID_j^k\|K_1)$，$M_3'=h(SID_j^k\|K_1\|X_{SN_j}^k\|r_g^{k'})$，比较$M_3'$与$M_3$. 若相等，则继续后续计算；否则，终止该会话.

V5. SN_j^k选择k_j，然后计算$K_3=r_j\cdot P_k$，$K_4=r_j\cdot K_1$，$M_5=h(r_g^{k'}\|K_3\|X_{SN_j}^k\|SID_j^k\|K_1)$，以及与${U_i}^k$的会话密钥$SK=h(K_1\|K_3\|K_4\|SID_j^k)$.

V6. $SN_j^k\rightarrow GWN_k$：$MSG_3=\{M_5, K_3\}$.

V7. GWN_k计算$M_5'=h(r_g^k\|K_3\|X_{SN_j}^{k'}\|SID_j^{k'}\|K_1)$，

用户 U_i^k $\{A_i, B_i, a, \delta_i, Y_k, P_k\}$	网关 GWN_k $X_{shar}, \{X_{GWN}^k, GID_k\}, \{ID_i^k, T_{rg_i}\}$ and $\{SID_j^k\}$	传感器节点 SN_j^k $\{SID_j^k, X_{SN_j}^k = h(SID_j^k \| \| X_{GWN}^k)\}$
用户注册阶段		
输入 (ID_i^k, PW_i^k, Bio_i) 选择一个随机数 a' 计算: $Gen(Bio_i) = (\delta_i, \tau_i)$ $RPW_i' = h(PW_i \| \| \delta_i \| \| a')$	计算: $X_{U_i}^k = h(ID_i^k \| \| X_{GWN}^k \| \| T_{rg_i})$ $B_i' = h(RPW_i' \| \| ID_i^k) \oplus X_{U_i}^k$ 存储 $\{ID_i^k, T_{rg_i}, Honey - list = 0\}$	
$\{ID_i^k, RPW_i'\}$ ⟹	⟸ 存储了 $\{B_i', Y_k, P_k\}$的智能卡	
选择一个随机数 a $X_{U_i}^k = B_i' \oplus h(RPW_i \| \| ID_i^k)$ $A_i = h(ID_i^k \| \| PW_i^k \| \| \delta_i \| \| X_{U_i}^k) mod\ n_0$ $RPW_i = h(PW_i^k \| \| \delta_i \| \| a)$ $B_i = X_{U_i}^k \oplus h(RPW_i \| \| ID_i^k)$ 存储 $\{A_i, B_i, a, \tau_i, Y_k, P_k\}$		
登录及认证阶段		
输入 (ID_i^k, PW_i^k, Bio_i) $\delta_i^* = Ren(Bio_i, \tau_i)$ $RPW_i^* = h(PW_i^k \| \| \delta_i^* \| \| a)$ $X_{U_i}^k = B_i \oplus h(RPW_i^* \| \| ID_i^k)$ $A_i^* = h(ID_i^k \| \| PW_i^k \| \| \delta_i \| \| X_{U_i}^k) mod\ n_0$ $A_i^* \stackrel{?}{=} A_i$ 选择随机数 r_i $K_1 = r_i \cdot P_k$ $K_2 = r_i \cdot Y_k$ $M_1 = h(X_{U_i}^k \| \| ID_i^k \| \| K_1 \| \| K_2)$ $M_2 = ID_i^k \oplus h(K_1 \| \| K_2)$ $EID_j = SID_j^k \oplus h(ID_i^k \| \| K_2)$	计算: $K_2' = X_{GWN}^k \cdot K_1$ $ID_i^{k\prime} = M_2 \oplus h(K_1 \| \| K_2)$ $X_{U_i}^{k\prime} = h(ID_i^{k\prime} \| \| X_{GWN}^k \| \| T_{rg_i})$ $M_1' = h(X_{U_i}^{k\prime} \| \| ID_i^{k\prime} \| \| K_1 \| \| K_2')$ $M_1' \stackrel{?}{=} M_1$ 选择 r_g^k $SID_j^{k\prime} = EID_j \oplus h(ID_i^{k\prime} \| \| K_2)$ $X_{SN_j}^{k\prime} = h(SID_j^{k\prime} \| \| X_{GWN}^k)$ $M_3 = h(SID_j^{k\prime} \| \| K_1 \| \| X_{SN_j}^{k\prime} \| \| r_g^k)$ $M_4 = r_g^k \oplus h(X_{SN_j}^{k\prime} \| \| SID_j^{k\prime} \| \| K_1')$	$r_g^{k\prime} = M_4 \oplus h(X_{SN_j}^k \| \| SID_j^k \| \| K_1)$ $M_3' = h(SID_j^k \| \| K_1 \| \| X_{SN_j}^k \| \| r_g^{k\prime})$ $M_3' \stackrel{?}{=} M_3$ 选择 k_j, 计算: $K_3 = r_j \cdot P_k$ $K_4 = r_j \cdot K_1$ $M_5 = h(r_g^{k\prime} \| \| K_3 \| \| X_{SN_j}^k \| \| SID_j^k \| \| K_1)$ $SK = h(K_1 \| \| K_3 \| \| K_4 \| \| SID_j^k)$
$MSG_1 = \{K_1, M_1, M_2, EID_j\}$ ⟹	$MSG_2 = \{K_1, M_3, M_4\}$ ⟹	⟸ $MSG_3 = \{M_5, K_3\}$
$M_6^* = h(X_{U_i}^k \| \| K_1 \| \| K_2 \| \| ID_i^k \| \| SID_j^k \| \| K_3)$ $M_6^* \stackrel{?}{=} M_6$ $K_4^* = r_i \cdot K_3$ $SK = h(K_1 \| \| K_3 \| \| K_4^* \| \| SID_j^k)$	$M_5' = h(r_g^k \| \| K_3 \| \| X_{SN_j}^{k\prime} \| \| SID_j^{k\prime} \| \| K_1)$ $M_5' \stackrel{?}{=} M_5$ $M_6 = h(X_{U_i}^{k\prime} \| \| K_1 \| \| K_2' \| \| ID_i^k \| \| SID_j^{k\prime} \| \| K_3)$ ⟸ $MSG_4 = \{M_6, K_3\}$	

图2　本文改进协议在场景1的认证流程

然后比较M_5'与M_5的大小,若相等,则继续后面的计算;否则,终止该会话.

V7. 计算$M_6 = h(X_{U_i}^{k'} \| K_1 \| K_2' \| ID_i^k \| SID_j^{k'} \| K_3)$.

V8. $GWN_k \rightarrow U_i^k$: $MSG_4 = \{M_6, K_3\}$. U_i^k计算$M_6^* = h(X_{U_i}^k \| K_1 \| K_2 \| ID_i^k \| SID_j^k \| K_3)$,比较$M_6^*$与$M_6$,若相等,则继续;否则,终止会话.

V9. 计算$K_4^* = r_i \cdot K_3$,以及与传感器节点SN_j^k共享的会话密钥$SK = h(K_1 \| K_3 \| K_4^* \| SID_j^k)$.

7.7　场景2的认证与密钥协商阶段

如图2,场景2中,假设用户U_i^1所在的网关为GWN_1(即本地网关$HGWN$),该用户想访问的目标传感器节点为SN_j^2(处于网关GWN_2的覆盖范围内). 因此,在用户登录阶段,用户相关的参数k实例化为1,传感器节点相关参数k实例化为2.

V1. GWN_1计算$K_2' = X_{GWN}^1 \cdot K_1$, $ID_i^{1'} = M_2 \oplus h(K_1 \| \| K_2')$, $X_{U_i}^{1'} = h(ID_i^{1'} \| X_{GWN}^1 \| T_{rg_i})$, $M_1' = h(X_{U_i}^{1'} \| ID_i^{1'} \| K_1 \| K_2')$. 比较$M_1'$与$M_1$,若相等,则继续;否则,终止会话,且令honey-list= honey-list+1,且一旦honey-list的值超过10,则冻结该用户的账户,直至U_i^1重注册.

V2. GWN_1选择r_g^1,计算$SID_j^{2'} = EID_j \oplus h(ID_i^{1'} \| K_2)$,$ID_i = h(ID_i^{1'} \| r_g^1)$,$M_3 = h(SID_j^{2'} \| K_1 \| S_{ran} \| r_g^1 \| TID_i)$,

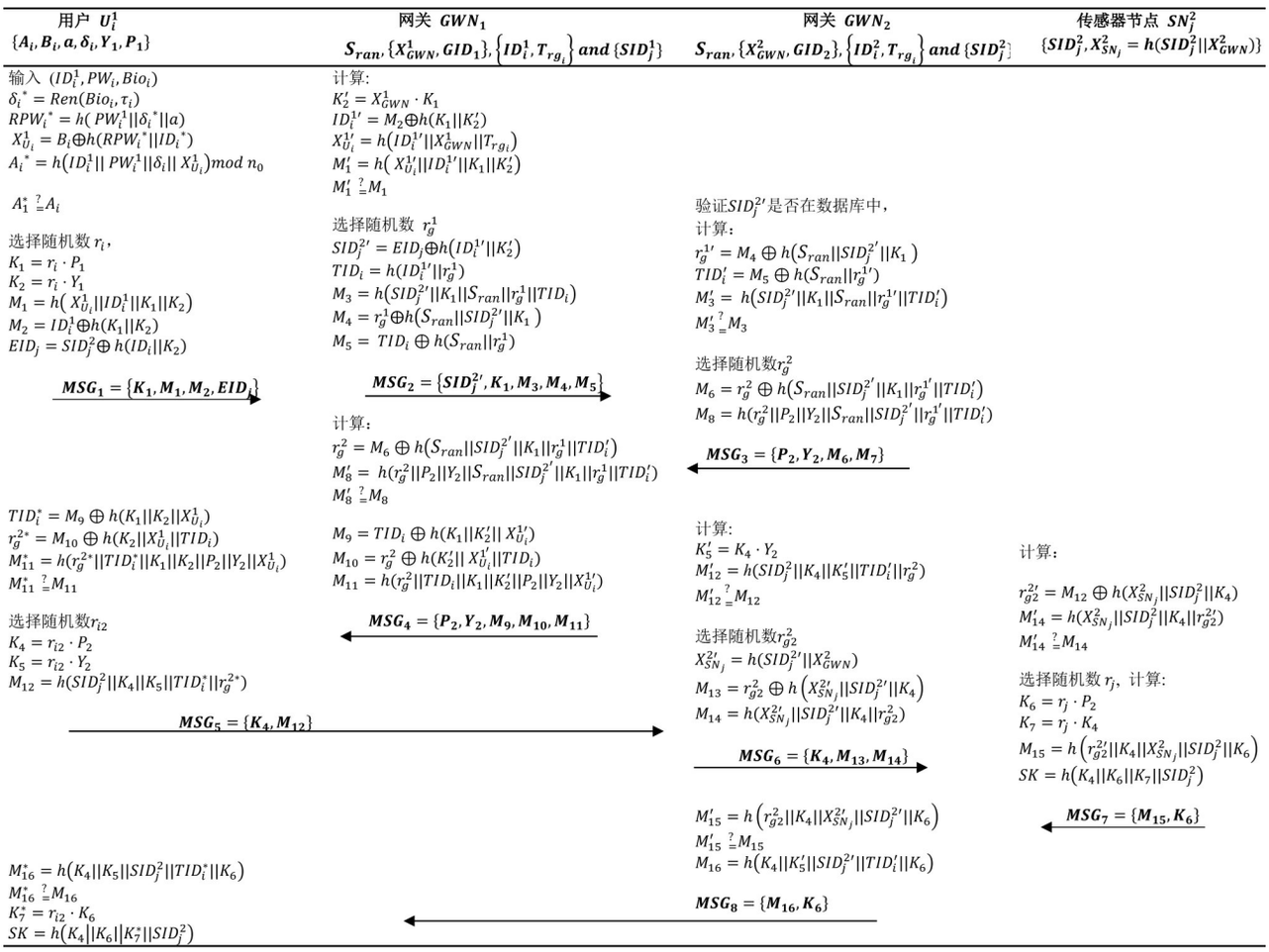

图3 本文改进协议在场景2的认证流程

$M_4 = r_g^1 \oplus h(S_{ran}||SID_j^{2'}||K_1), M_5 = TID_i \oplus h(S_{ran}||r_g^1)$.

V3. $GWN_1 \rightarrow GWN_2$: $MSG_2 = \{SID_j^{2'}, K_1, M_3, M_4, M_5\}$. GWN_1 广播 MSG_2, GWN_2 判断 $SID_j^{2'}$ 是否在自身区域内,然后对消息进行响应.

V4. GWN_2 检查 $SID_j^{2'}$ 对应的节点是否在自身区域中,计算 $r_g^{1'} = M_4 \oplus h(S_{ran}||SID_j^{2'}||K_1)$, $TID_i' = M_5 \oplus h(S_{ran}||r_g^{1'}), M_3' = h(SID_j^{2'}||K_1||S_{ran}||r_g^{1'}||TID_i')$. 比较 M_3' 与 M_3,若相等,则继续后面的计算;否则,终止该会话.

V5. GWN_2 选择随机数 r_g^2,然后计算 $M_6 = r_g^2 \oplus h(S_{ran}||SID_j^{2'}||K_1||r_g^{1'}||TID_i'), M_8 = h(r_g^2||P_2||Y_2||S_{ran}||SID_j^{2'}||K_1||r_g^{1'}||TID_i')$.

V6. $GWN_2 \rightarrow GWN_1$: $MSG_3 = \{P_2, Y_2, M_6, M_8\}$

V7. GWN_1 首先计算 $r_g^2 = M_6 \oplus h(S_{ran}||SID_j^{2'}||K_1||r_g^1||TID_i'), M_8' = h(r_g^2||P_2||Y_2||S_{ran}||SID_j^{2'}||K_1||r_g^{1'}||TID_i')$,然后对比 M_8' 与 M_8 的大小,若相等,则继续后面的计算;否则,终止该会话.

V8. GWN_1 计算 $M_9 = TID_i \oplus h(K_1||K_2'||X_{U_i}^{1'}), M_{10} = r_g^2 \oplus h(K_2'||X_{U_i}^{1'}||TID_i'), \quad M_{11} = h(r_g^2||TID_i||K_1||K_2'||P_2||Y_2||X_{U_i}^{1'})$.

V9. $GWN_1 \rightarrow U_i^1$: $MSG_4 = \{P_2, Y_2, M_9, M_{10}, M_{11}\}$.

V10. U_i^1 计算 $TID_i^* = M_9 \oplus h(K_1||K_2||X_{U_i}^1), r_g^{2*} = M_{10} \oplus h(K_2||X_{U_i}^1||TID_i), M_{11}^* = h(r_g^{2*}||TID_i^*||K_1||K_2||P_2||Y_2||X_{U_i}^1)$. 比较 M_{11}^* 与 M_{11} 的大小,若相等,则继续后续计算;否则,终止会话.

V11. U_i^1 选择随机数 r_{i2},计算 $K_4 = r_{i2} \cdot P_1, K_5 = r_{i2} \cdot Y_1, M_{12} = h(SID_j^2||K_4||K_5||TID_i^*||r_g^{2*})$.

V12. $U_i^1 \rightarrow GWN_2$: $MSG_5 = \{K_4, M_{11}\}$.

V13. GWN_2 计算 $K_5' = K_4 \cdot Y_2$, $M_{12}' = h(SID_j^2||K_4||K_5||TID_i'||r_g^2)$,比较 M_{12}' 与 M_{12},若相等,则继续后面的计算;否则,终止该会话.

V14. GWN_2 选择 $r_{g^2}^2$,计算 $X_{SN_j}^{2'} =$

$h(SID_j^{2'}\|X_{GWN}^2)$, $M_{13}=r_{g^2}^2\oplus h(X_{SN_j}^{2'}\|SID_j^{2'}\|K_4)$, $M_{14}=h(X_{SN_j}^{2'}\|SID_j^{2'}\|K_4\|r_{g^2}^2)$.

V15. SN_j^2 计算 $r_{g^2}^{2'}=M_{12}\oplus h(X_{SN_j}^2\|SID_j^2\|K_4)$, $M_{14}'=h(X_{SN_j}^2\|SID_j^2\|K_4\|r_{g^2}^{2'})$. 比较 M_{14}' 与 M_{14}, 若相等,则继续;否则,终止会话.

V16. SN_j^2 选择随机 r_j, 计算 $K_6=r_j\cdot P_2$, $K_7=r_j\cdot K_4$, $M_{15}=h(r_{g^2}^{2'}\|K_4\|X_{SN_j}^2\|SID_j^2\|K_6)$, 以及会话密钥 $SK=h(K_4\|K_6\|K_7\|SID_j^2)$.

V17. $SN_j^2\rightarrow GWN_2$: $MSG_7=\{M_{15},K_6\}$.

V18. GWN_2 计算 $M_{15}'=h(r_{g^2}^2\|K_4\|X_{SN_j}^{2'}\|SID_j^{2'}\|K_6)$, 然后对比 M_{15}' 与 M_{15} 的大小,若相等,则继续后面的计算;否则,终止该会话.

V19. GWN_2 计算 $M_{16}=h(K_4\|K_5'\|SID_j^{2'}\|TID_i'\|K_6)$.

V20. $GWN_1\rightarrow U_i^{\,1}$: $MSG_8=\{M_{16},M_6\}$.

V21. $U_i^{\,1}$ 计算 $M_{16}^*=h(K_4\|K_5\|SID_j^2\|TID_i^*\|K_6)$, 比较 M_{16}^* 与 M_{16} 的大小,若相等,则继续后面的计算;否则,终止该会话.

V22. $U_i^{\,1}$ 计算 $K_7{}^*=r_{i2}\cdot K_6$, 以及与 SN_j^2 之间的会话密钥 $SK=h(K_4\|K_6\|K_7{}^*\|SID_j^2)$.

7.8　口令更新阶段

U1. $U_i^{\,k}$ 输入 $\{ID_i^k,PW_i^k,Bio_i,Bio_i^{new}\}$.

U2. 智能卡计算 $\delta_i^*=Rep(Bio_i,\tau_i)$, $RPW_i^*=h(PW_i^k\|\delta_i^*\|a)$, $X_{U_i}^k=B_i\oplus h(RPW_i^*\|ID_i^k)$, $A_i{}^*=h(ID_i^k\|PW_i^k\|\delta_i{}^*\|X_{U_i}^k)\bmod n_0$. 比较 $A_i{}^*$ 与 A_i 的大小,若相等,则继续;否则,终止该会话.

U3. 智能卡接受请求,计算新的参数 $RPW_i^{new}=h(PW_i^{new}\|\delta_i{}^*\|a)$, $B_i^{new}=h(RPW_i^{new}\|ID_i^k)\oplus X_{U_i}^k$, $A_i{}^{new}=h(ID_i^k\|PW_i^{new}\|X_{U_i}^k)\bmod n_0$, 然后将卡中 $\{A_i,B_i\}$ 更新为 $\{A_i{}^{new},B_i^{new}\}$.

7.9　用户重注册阶段

当登录失败次数超过一定阈值,本协议会自动冻结用户账户,以降低攻击者攻击成功的概率. 如用户账号被冻结,可通过如下步骤激活:

RR1. $U_i^{\,k}\Rightarrow GWN_k$: $\{ID_i^k,RPW_i',$重注册请求$\}$. $U_i^{\,k}$ 输入 $\{ID_i^k,PW_i^k,Bio_i\}$, 选择随机数 a', 计算: $Gen(Bio_i)=(\delta_i,\tau_i)$, $RPW_i'=h(PW_i\|\delta_i\|a')$.

RR2. GWN_k 检查 ID_i^k 是否在数据库中. 若不在,终止会话;否则计算 $X_{U_i}^k=h(ID_i^k\|X_{GWN}^k\|T_{rg_i}')$, $B_i'=h(RPW_i'\|ID_i^k)\oplus X_{U_i}^k$, 将 $\{ID_i^k,T_{rg_i}',$honey-list$=0\}$ 存储在数据库中, T_{rg_i}' 是当前时间戳.

RR3. $GWN_k\Rightarrow U_i^{\,k}$:智能卡 $\{B_i',Y_k,P_k\}$.

RR4. $U_i^{\,k}$ 选择一个随机数 a, 然后计算 $X_{U_i}^k=B_i'\oplus h(RPW_i\|ID_i^k)$, 以及 $A_i=h(ID_i^k\|PW_i^k\|\delta_i\|X_{U_i}^k)\bmod n_0$, $RPW_i=h(PW_i^k\|\delta_i\|a)$, $B_i=h(RPW_i\|ID_i^k)\oplus X_{U_i}^k$, 并将 $\{A_i,B_i,a,\tau_i,Y_k,P_k\}$ 存储到智能卡中.

7.10　动态传感器节点增加阶段

若新传感器节点 SN_j^k 想要加入网关 GWN_k, SN_j^k 只需如节7.3所述向网关发起注册请求. SN_j^k 成功注册后, GWN_k 广播 $\{SID_j^k\oplus h(S_{ran}\|r_k),r_k\}$ 给其他网关,以传递 SN_j^k 的身份标识 SID_j^k.

8　安全性分析

本小节采用BAN逻辑[22]对协议的安全性进行分析,BAN逻辑的符号及规则如表3所示.

表3　BAN逻辑的符号及规则

P,Q	通信方
X,Y	参数
K	密钥
$P\lhd X$	P收到了包含X的消息
$P\|\sim X$	P发送了包含X的消息
$P\|\equiv X$	P相信X
$P\overset{Y}{\Leftrightarrow}Q$	P和Q共享秘密X
$\#(X)$	X是新鲜的
$P\overset{K}{\leftrightarrow}Q$	P和Q共享密钥K
$\{X\}_K$	使用对X进行加密
$<X>_Y$	X包含秘密Y
$P\Rightarrow X$	P拥有对X正确与否的判决权
消息意义规则	$\dfrac{P\|\equiv P\overset{K}{\leftrightarrow}Q,P\lhd\{X\}_K}{P\|\equiv Q\|\sim X}$或 $\dfrac{P\|\equiv P\overset{Y}{\Leftrightarrow}Q,P\lhd<X>_Y}{P\|\equiv Q\|\sim X}$
信念规则	$\dfrac{P\|\equiv X,P\|\equiv Y}{P\|\equiv(X,Y)}$
随机数验证规则	$\dfrac{P\|\equiv\#(X),P\|\equiv Q\|\sim X}{P\|\equiv Q\|\equiv X}$
仲裁规则	$\dfrac{P\|\equiv Q\Rightarrow X,P\|\equiv Q\|\equiv X}{P\|\equiv X}$

8.1　场景1的安全性分析

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: $SN_j^k|\equiv U_i^{\,k}|\equiv(U_i^{\,k}\overset{SK}{\longleftrightarrow}SN_j^k)$

G2: $SN_j^k|\equiv(U_i^{\,k}\overset{SK}{\longleftrightarrow}SN_j^k)$

G3: $U_i^{\,k}|\equiv SN_j^k|\equiv(U_i^{\,k}\overset{SK}{\longleftrightarrow}SN_j^k)$

G4: $U_i^{\,k}|\equiv(U_i^{\,k}\overset{SK}{\longleftrightarrow}SN_j^k)$

消息的理想化形式：

MSG_1: ${U_i}^k \rightarrow GWN_k < ID_i^k, SID_j^k, K_1 >_{X_{U_1}^k}$

MSG_2: $GWN_k \rightarrow SN_j^k < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >_{X_{SN_j}^k}$

MSG_3: $SN_j^k \rightarrow GWN_k < SID_j^k, K_1, r_g^k, K_3 >_{X_{SN_j}^k}$

MSG_4: $GWN_k \rightarrow {U_i}^k < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >_{X_{U_1}^k}$

协议的初始化假设：

A1: $GWN_k| \equiv {U_i}^k \overset{X_{U_1}^k}{\longleftrightarrow} GWN_k$

A2: $GWN_k| \equiv \#(K_1)$

A3: $GWN_k| \equiv {U_i}^k \Rightarrow < ID_i^k, SID_j^k, K_1 >$

A4: $SN_j^k| \equiv GWN_k \overset{X_{SN_j}^k}{\longleftrightarrow} SN_j^k$

A5: $SN_j^k| \equiv \#(K_1)$

A6: $SN_j^k| \equiv GWN_k \Rightarrow < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >$

A7: $SN_j^k| \equiv {U_i}^k \Rightarrow ({U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k)$

A8: $GWN_k| \equiv GWN_k \overset{X_{SN_j}^k}{\longleftrightarrow} SN_j^k$

A9: $GWN_k| \equiv \#(K_3)$

A10: ${U_i}^k| \equiv {U_i}^k \overset{X_{U_1}^k}{\longleftrightarrow} GWN_k$

A11: ${U_i}^k| \equiv \#(K_2)$

A12: ${U_i}^k| \equiv GWN_k \Rightarrow < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >$

A13: ${U_i}^k| \equiv SN_j^k \Rightarrow ({U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k)$

从消息MSG_1，我们得到

(1) $GWN_k \lhd < ID_i^k, SID_j^k, K_1 >_{X_{U_1}^k}$

根据(1)，A1，应用消息意义规则，得到

(2) $GWN_k| \equiv {U_i}^k| \sim < ID_i^k, SID_j^k, K_1 >$

根据(2)，A2，应用随机数验证规则，得到

(3) $GWN_k| \equiv {U_i}^k| \equiv < ID_i^k, SID_j^k, K_1 >$

根据(3)，A3，应用仲裁规则，得到

(4) $GWN_k| \equiv < ID_i^k, SID_j^k, K_1 >$

从消息MSG_2，得到

(5) $SN_j^k \lhd < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >_{X_{SN_j}^k}$

根据(5)，A4，应用消息意义规则，得到

(6) $SN_j^k| \equiv GWN_k| \sim < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >$

根据(6)，A5，应用随机数验证规则，得到

(7) $SN_j^k| \equiv GWN_k| \equiv < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >$

根据(7)，A6，应用仲裁规则，得到

(8) $SN_j^k| \equiv < SID_j^k, {U_i}^k| \equiv K_1, r_g^k >$

根据(8)，以及$SK = h(K_1 \| K_3 \| r_j \cdot K_1 \| SID_j^k)$，得到

(9) $SN_j^k| \equiv {U_i}^k| \equiv ({U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k)$

根据(9)，A7，应用仲裁规则，得到

(10) $SN_j^k| \equiv ({U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k)$

从消息MSG_3，我们得到

(11) $GWN_k \lhd < SID_j^k, K_1, r_g^k, K_3 >_{X_{SN_j}^k}$

根据(11)，A8，应用消息意义规则，得到

(12) $GWN_k| \equiv SN_j^k| \sim < SID_j^k, K_1, K_3 >$

根据(12)，A9，应用随机数验证规则，得到

(13) $GWN_k| \equiv SN_j^k| \equiv < SID_j^k, K_1, K_3 >$

从消息MSG4，我们得到

(13) ${U_i}^k \lhd < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >_{X_{U_1}^k}$

根据(13)，A10，应用消息意义规则，得到

(14) ${U_i}^k| \equiv GWN_k| \sim < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >$

根据(14)，A11，应用随机数验证规则，得到

(15) ${U_i}^k| \equiv GWN_k| \equiv < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >$

根据(15)，A12，应用仲裁规则，得到

(16) ${U_i}^k| \equiv < SID_j^k, SN_j^k| \equiv K_1, SN_j^k| \equiv K_3 >$

根据(16)，以及$SK = h(K_1 \| K_3 \| r_j \cdot K_1 \| SID_j^k)$，得到

(17) ${U_i}^k| \equiv SN_j^k| \equiv {U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k$

根据(17)，A13，应用仲裁规则，得到

(18) ${U_i}^k| \equiv {U_i}^k \overset{SK}{\longleftrightarrow} SN_j^k$

8.2 场景2的安全性分析

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: ${U_i}^1| \equiv SN_j^2| \equiv ({U_i}^1 \overset{SK}{\longleftrightarrow} SN_j^2)$

G2: ${U_i}^1| \equiv ({U_i}^1 \overset{SK}{\longleftrightarrow} SN_j^2)$

G3: $SN_j^2| \equiv {U_i}^1| \equiv ({U_i}^1 \overset{SK}{\longleftrightarrow} SN_j^2)$

G4: $SN_j^2| \equiv ({U_i}^1 \overset{SK}{\longleftrightarrow} SN_j^2)$

消息的理想化形式：

MSG_2: $GWN_1 \rightarrow GWN_2 < SID_j^2, K_1, r_g^1, {U_i}^1 \overset{TID_i}{\longleftrightarrow} GWN_2 >_{S_{ran}}$

MSG_4: $GWN_1 \rightarrow {U_i}^1 < r_g^2, {U_i}^1 \overset{TID_i}{\longleftrightarrow} GWN_2, K_1 >_{X_{U_1}^2}$

MSG_5: ${U_i}^1 \rightarrow GWN_2 < SID_j^2, K_4, r_g^{2*} >_{TID_i}$

MSG_6: $GWN_2 \rightarrow SN_j^2 < {U_i}^1| \equiv K_4, SID_j^{2'}, r_{g^2}^2 >_{X_{SN_j}^2}$

MSG_7: $SN_j^2 \rightarrow GWN_2 < r_{g^2}^{2'}, K_4, SID_j^2, K_6 >_{X_{SN_j}^2}$

MSG_8: $GWN_2 \rightarrow {U_i}^1 < SN_j^2| \equiv K_4, SID_j^2, SN_j^2| \equiv K_6 >_{TID_i}$

协议的初始化假设:

A1: $GWN_2|\equiv GWN_2 \xleftrightarrow{S_{ran}} GWN_1$

A2: $GWN_2|\equiv \#(K_1)$

A3: $GWN_2|\equiv GWN_1 \Rightarrow U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

A4: $U_i{}^1 \xleftrightarrow{X_{U_1}^k} GWN_1$

A5: $U_i{}^1|\equiv \#(K_1)$

A6: $U_i{}^1|\equiv GWN_1 \Rightarrow U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

A7: $GWN_2|\equiv \#(K_4)$

A8: $GWN_2|\equiv U_i{}^1 \Rightarrow <SID_j^2, K_4, r_g^{2*}>$

A9: $SN_j^2|\equiv GWN_2 \xleftrightarrow{X_{SN_j}^k} SN_j^2$

A10: $SN_j^2|\equiv \#(K_4)$

A11: $SN_j^2|\equiv GWN_2 \Rightarrow <U_i{}^1 \equiv K_4, SID_j^{2'}, r_{g^2}^2>$

A12: $SN_j^2|\equiv U_i{}^1 \Rightarrow (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

A13: $GWN_2|\equiv GWN_2 \xleftrightarrow{X_{SN_j}^k} SN_j^2$

A14: $GWN_2|\equiv \#(K_6)$

A15: $U_i{}^1|\equiv \#(K_6)$

A16: $U_i{}^1|\equiv GWN_2 \Rightarrow <SN_j^2|\equiv K_4, SN_j^2|\equiv K_6, SID_j^2>$

A17: $U_i{}^1|\equiv SN_j^2 \Rightarrow (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

从消息MSG_2,我们得到

(1) $GWN_2 \lhd < SID_j^2, K_1, r_g^1, U_i{}^1 \xleftrightarrow{TID_i} GWN_2 >_{S_{ran}}$

根据(1), A1,应用消息意义规则,得到

(2) $GWN_2|\equiv GWN_1|\sim <SID_j^2, K_1, r_g^1, U_i{}^1 \xleftrightarrow{TID_i} GWN_2>$

根据(2), A2,应用随机数验证规则,得到

(3) $GWN_2|\equiv GWN_1|\equiv U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

根据(3), A3,应用仲裁规则,得到

(4) $GWN_2|\equiv U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

从消息MSG_4,我们得到

(5) $U_i{}^1 \lhd < r_g^2, U_i{}^1 \xleftrightarrow{TID_i} GWN_2, K_1 >_{X_{U_1}^2}$

根据(1), A4,应用消息意义规则,得到

(6) $U_i{}^1|\equiv GWN_1|\sim <r_g^2, U_i{}^1 \xleftrightarrow{TID_i} GWN_2, K_1>$

根据(2), A5,应用随机数验证规则,得到

(7) $U_i{}^1|\equiv GWN_1|\equiv U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

根据(3), A6,应用仲裁规则,得到

(8) $U_i{}^1|\equiv U_i{}^1 \xleftrightarrow{TID_i} GWN_2$

从消息MSG_5,我们得到

(9) $GWN_2 \lhd < SID_j^2, K_4, r_g^{2*} >_{TID_i}$

根据(9), (4),应用消息意义规则,得到

(10) $GWN_2|\equiv U_i{}^1|\sim <SID_j^2, K_4, r_g^{2*}>$

根据(10), A7,应用随机数验证规则,得到

(11) $GWN_2|\equiv U_i{}^1|\equiv <SID_j^2, K_4, r_g^{2*}>$

根据(11), A8,应用仲裁规则,得到

(12) $GWN_2|\equiv <SID_j^2, K_4, r_g^{2*}>$

从消息MSG6,我们得到

(13) $SN_j^2 \lhd < U_i{}^1|\equiv K_4, SID_j^{2'}, r_{g^2}^2 >_{X_{SN_j}^2}$

根据(13), A9,应用消息意义规则,得到

(14) $SN_j^2|\equiv GWN_2|\sim <U_i{}^1|\equiv K_4, SID_j^{2'}, r_{g^2}^2>$

根据(14), A10,应用随机数验证规则,得到

(15) $SN_j^2|\equiv GWN_2|\equiv <U_i{}^1|\equiv K_4, SID_j^{2'}, r_{g^2}^2>$

根据(15), A11,应用仲裁规则,得到

(16) $SN_j^2|\equiv <U_i{}^1|\equiv K_4, SID_j^{2'}, r_{g^2}^2>$

根据(16), 以及 $SK = h(K_4 \| K_6 \| r_j \cdot K_4 \| SID_j^2)$,得到

(17) $SN_j^2|\equiv U_i{}^1|\equiv (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

根据(17), A12,应用仲裁规则,得到

(18) $SN_j^2|\equiv (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

从消息MSG_7,我们得到

(19) $GWN_2 \lhd < r_{g^2}^{2'}, K_4, SID_j^2, K_6 >_{X_{SN_j}^2}$

根据(19), A13,应用消息意义规则,得到

(20) $GWN_2|\equiv SN_j^2|\sim <r_{g^2}^{2'}, K_4, SID_j^2, K_6>$

根据(20), A14,应用随机数验证规则,得到

(21) $GWN_2|\equiv SN_j^2|\equiv <r_{g^2}^{2'}, K_4, SID_j^2, K_6>$

从消息MSG_8,我们得到

(22) $U_i{}^1 \lhd GWN_2 < SN_j^2|\equiv K_4, SID_j^2, SN_j^2|\equiv K_6 >_{TID_i}$

根据(22), (8),应用消息意义规则,得到

(23) $U_i{}^1|\equiv GWN_2|\sim <SN_j^2|\equiv K_4, SID_j^2, SN_j^2|\equiv K_6>$

根据(23), A15,应用随机数验证规则,得到

(24) $U_i{}^1|\equiv GWN_2|\equiv <SN_j^2|\equiv K_4, SID_j^2, SN_j^2|\equiv K_6>$

根据(24), A16,应用仲裁规则,得到

(25) $U_i{}^1|\equiv <SN_j^2|\equiv K_4, SID_j^2, SN_j^2|\equiv K_6>$

根据(25), 以及 $SK = h(K_4 \| K_6 \| r_j \cdot K_4 \| SID_j^2)$,得到

(26) $U_i{}^1|\equiv SN_j^2|\equiv (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

根据(26), A17,应用仲裁规则,得到

(27) $U_i{}^1|\equiv (U_i{}^1 \xleftrightarrow{SK} SN_j^2)$

9　启发式安全性分析

本节采用启发式分析的方式来分析一些重要的安全目标.

9.1 离线字典猜测攻击

基于智能卡非抗窜扰的假设,攻击者$\mathcal{A}$可获取智能卡中的参数,用猜测的口令和身份标识来构造验证因子,并通过对比构造的验证因子与真实验证因子的值来验证猜测的口令的正确性. 在改进的协议中,假设$\mathcal{A}$得到了生物特征Bio_i以及智能卡中的数据,并按照节6.1步骤,成功找到了满足条件$(A_i^* = A_i)$的(ID_i^k, PW_i^k),但由于符合上述等式的口令和身份标识有约2^{32}个[17],$\mathcal{A}$只能通过线上登录来确认. 而由于honey-list记录了认证失败的次数,$\mathcal{A}$在线尝试次数有限(例如10次),仅通过10次在线猜测就得到口令的概率极小.

而为了执行离线字典猜测攻击II,攻击者需要构造出验证因子$M_1 = h(X_{U_i}^k \| ID_i^k \| K_1 \| K_2)$. 其中$X_{U_i}^k$可由猜测的$(ID_i^k, PW_i^k)$构造出来,但$K_2$是是通过公钥技术计算出来的参数,除了用户$U_i$外,只有拥有私钥$X_{GWN}^k$的网关才能够计算$X_{GWN}^k \cdot K_1$得到$K_2$. 因而改进的协议能抵抗离线字典猜测攻击II.

9.2 用户匿名

用户匿名要求攻击者无法计算出用户的身份标识,也无法从众多的会话中判断某一特定用户的会话. 改进的协议采用公钥技术来实现用户匿名:一方面,用户的身份标识ID_i^k不直接暴露在公开信道中,而通过公钥密码技术计算得到的K_2来保护ID_i^k. 如9.1节所述,除用户外,只有拥有私钥的网关才能用的K_1计算K_2,因而攻击者无法计算出ID_i^k;另一方面,K_1、K_2和M_2在每轮会话中都不同,攻击者无法通过M_2追踪用户U_i的会话.

9.3 前向安全

本文基于椭圆曲线的Diffie-Hellman密钥交换算法的基本思想设计了安全的密钥交换协议. 改进的协议的会话密钥$SK = h(K_1 \| K_3 \| K_4 \| SID_j^k)$,其中$K_4 = r_i \cdot K_3 = r_i \cdot r_j \cdot P_k$. 对攻击者来说,他只能够通过窃听公开信道得到$K_1$和$K_3$以及$P_k$. 而已知这些参数计算,是一个决策性Diffie-Hellman(DDH)困难问题,攻击者无法在多项式时间内计算出来. 因而改进的协议能够实现前向安全.

9.4 双向认证

以场景1为例,网关与用户之间通过秘密参数K_2和$X_{U_i}^k$进行相互认证. 具体来说,网关通过验证计算出来M_1'是否等于用户发送的M_1来认证用户的身份;用户通过验证计算出来M_6'是否等于网关发送的M_6来认证网关的身份. 网关与传感器节点之间通过秘密参数$X_{SN_j}^k$和随机数r_g^k进行相互认证. 具体来说,网关通过验证计算出来M_5'是否等于传感器节点发送的M_5来认证传感器节点的身份;传感器节点通过验证计算出来M_3'是否等于网关发送的M_3来认证网关的身份. 而用户与传感器节点之间的认证通过对网关的认证完成.

9.5 内部攻击

内部攻击指用户在向网关注册的过程中,泄漏了敏感信息,使得网关管理员能够有优势执行口令猜测的攻击. 假设攻击者$\mathcal{A}$获得了用户$U_i{}^k$的注册信息$\{ID_i^k, RPW_i'\}$,还同时获取了$U_i{}^k$的生物特征和智能卡中的参数. 按照第4.4节所述,$\mathcal{A}$需计算RPW_i',因$RPW_i' = h(PW_i^k \| \delta_i \| a')$,$\mathcal{A}$进而需得到$a'$的值. 但用户在拿到智能卡后,已经将$a'$替换为$a$,此时由智能卡中的参数无法推导出$a'$. 因而攻击者无法执行口令猜测的攻击.

10 与相关协议的对比分析

本节从安全性和性能两个方面对相关的协议进行对比分析,结果如表4和表5所示.

表4 多网关下用户认证协议的性能比较

协议	计算量/s			通信量/bit			存储量/bit		
	用户端	网关	传感器	用户	网关	传感器	用户端	网关	传感器
Xu等协议[24]	$5T_H + T_B$	$12T_H$	$4T_H$	768	896	256	512	2304	256
Guo等协议[25]	$6T_H + T_B$	$16T_H$	$6T_H$	896	1280	384	640	2432	384
Ali等协议[7]	$6T_H + 2T_S + T_B$	$6T_H + 2T_S$	$5T_H + T_S$	512	640	384	512	2048	256
Srinivas等协议[5]	$8T_H + T_B$	$6T_H$	$13T_H$	640	1280	384	512	2432	256
Wu等协议[14]	$8T_H$	$10T_H$	$3T_H$	869	1280	384	640	2432	256
Amin等协议[13]	$7T_H$	$8T_H$	$5T_H$	768	1280	384	512	2432	256
本文改进协议	$5T_H + T_B + 2T_P$	$9T_H + T_P$	$4T_H + 2T_P$	416	704	288	832	1696	256

T_H、T_S和T_P分别表示哈希运算、对称加解密、椭圆曲线点乘和生物特征运算花费的时间,"$\oplus$"和"$\|$"可忽略.

表5 多网关下用户认证协议的安全性比较

协议	年份	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
Xu等协议[24]	2019	是	否	否	否	否	否	是	是	是	是	否
Guo等协议[25]	2019	是	是	是	否	否	否	是	否	是	是	否
Ali等协议[7]	2018	是	是	否	否	否	否	是	否	是	否	否
Srinivas等协议[5]	2017	是	是	否	否	是	否	是	否	是	否	否
Wu等协议[14]	2017	是	是	否	否	否	否	是	否	是	是	否
Amin等协议[13]	2016	是	是	否	否	否	否	是	否	是	否	否
本文改进协议	2019	是	是	是	是	是	是	是	是	是	是	是

表4展示了相关协议的性能分析结果. 通信量主要指用户、传感器节点及网关之间相互传递的消息大小. 一般来说,假设哈希函数、随机数、时间戳、口令、身份标识等为128 bit;对基于对称密码算法的系统其长期秘密私钥为1024 bit,对基于ECC的系统其公私钥为160 bit;计算量指每次交互在各输入设备上执行计算所花费的时间;存储量表示用户、网关、传感器节点在本地存储的数据大小. 在认证协议中,注册阶段执行次数有限,协议的效率主要受到登录和认证阶段的影响;此外场景2的认证基于场景1,且发生频率不如场景1高,因而表4统计了如场景1下用户登录和认证阶段的计算量和通信量. 表4的对比显示,改进的协议牺牲了一定的计算量,这是因为协议使用了公钥密码技术,公钥密码技术的计算代价高于对称密码技术,但它是保证协议安全性的必要条件,能实现更好的安全性. 此外,改进协议的通信量和存储量与其他协议差别不大.

表5对比了几个协议的安全性,“是”表示该协议能够实现该指标,“否”表示不能. 从分析结果表明,本文协议克服了Ali等协议[7]和Srinivas等协议[5]的安全威胁,实现了2.2节提出的11个评价指标,而其他协议最多只能实现6个指标. 然而,改进的协议能抵抗无线传感网络中常见的智能卡丢失攻击和内部攻击,并实现了重要的前向安全性.

11 结束语

设计面向多网关的无线传感器网络多因素身份认证协议是近年来的研究热点. 本文分析了两个多网关环境的多因素身份认证协议,指出这两个协议存在多种安全威胁,提出了一个新的多因素认证协议. 对协议的安全性分析以及与其他协议的对比证明了新协议实现了更好的安全性.

需指出的是,现有协议假设网关是可信的,不会试图获取其他网关的敏感信息,然而实际中某个被攻击者腐化的网关可能是恶意的,在这种场景下如何实现用户身份认证,值得进一步研究.

参 考 文 献

[1] Wazid M. , Das A. K. , Odelu V. , Kumar N., Susilo W. Secure remote user authenticated key establishment protocol for smart home environment, IEEE Transactions on Dependable and Secure Computing, 2017. doi: 10.1109/TDSC.2017.2764083

[2] Kumari S, Om H. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks, 2016, 104(C): 137-154

[3] Gupta A, Tripathi M, Shaikh T J, .Sharma A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. Computer Networks, 2019, 149(A): 29-42

[4] Wazid M, Das A K, Odelu V, Kumar N, Conti M, Jo M. Design of secure user authenticated key management protocol for generic iot networks. IEEE Internet of Things Journal, 2017, 5(1): 269-282

[5] Srinivas J, Mukhopadhyay S, Mishra D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks, 2017, 54(A): 147-169

[6] Wang D, Li W, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics, 2018, 14(9): 4081-4092

[7] Ali R, Pal A K, Kumari S, Karuppiah M, Conti M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Generation Computer Systems, 2018, 84(C): 200-215

[8] Das M L. Two-factor user authentication in wireless sensor networks. IEEE transactions on wireless communications, 2009, 8(3): 1086-1090

[9] Khan M K, Alghathbar K. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. Sensors, 2010, 10(3): 2450-2459

[10] Chen T H, Shih W K. A robust mutual authentication protocol for wireless sensor networks. ETRI journal, 2010, 32(5): 704-712

[11] Vaidya B, Makrakis D, Mouftah H. Two - factor mutual authentication with key agreement in wireless sensor networks. Security and Communication Networks, 2016, 9(2): 171-183

[12] Turkanović M, Brumen B, Hölbl M. A novel user

authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks based on the Internet of Things notion. Ad Hoc Networks, 2014, 20(D): 96-112

[13] Amin R, Biswas G P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 2016, 36(A): 58-80

[14] Wu F, Xu L, Kumari S, Li X, Shen J, Choo K R, Wazid M, Das A K. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. Journal of Network and Computer Applications, 2017, 89(C): 72-85

[15] Wang C, Xu G, Sun J. An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. Sensors, 2017, 17(12): 2946

[16] Wang D, Cheng H, Wang P, Huang X Y, Guo G. Zipf's law in passwords. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776-2791

[17] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE transactions on dependable and secure computing, 2018, 15(4): 708-722

[18] 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)
(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,2019,30(8):2375-2391.)

[19] Wang D, He D, Wang P, Chu C H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing, 2014, 12(4): 428-442

[20] Ma C G, Wang D, Zhao S D. Security flaws in two improved remote user authentication schemes using smart cards. International Journal of Communication Systems, 2014, 27(10): 2215-2227

[21] Wang D, Li WT, Wang P. Crytanalysis of three anonymous authentication schemes for multi-server environment. Journal of Software, 2018, 29(7): 1937-1952 (in Chinese)
(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)

[22] Burrows M, Abadi M, Needham R M. A logic of authentication. //Proceedings of the twelfth ACM symposium on Operating systems principles, Litchfield Park, USA, 1989: 1-13

[23] Srinivas J, Das A K, Wazid M, et al. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Transactions on Dependable and Secure Computing, 2018. doi: 10.1109/TDSC.2018.2857811

[24] Xu L, Wu F. A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception. Arabian Journal for Science and Engineering, 2019, 44(2), 3977-3993

[25] Guo H, Gao Y, Xu T, Zhang X, Ye J. A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks. Ad Hoc Networks, 2019, 95(D): 101965

WANG Chen-Yu, Ph. D. candidate. Her research interests focus on security protocols.

WANG Ding, Ph. D. Professor. His research interests focus on authentication protocol and password security.

WENG Fei-Fei, Ph. D. candidate. Her research interest includes security protocols.

XU Guo-Ai, Professor. His research interests include information security and software security.

Background

This paper focuses on the security analysis of multi-factor user authentication for multi-gateway wireless sensor networks. Confronted with a powerful adversary, resource-constrained hardware and an impressive list of attributes, it is full of challenging in designing a user authentication scheme for multi-gateway environment. Recently, many authentication schemes for multi-gateway environment are proposed, but most of them are found insecure. In this paper, we analyze these two recent typical user authentication schemes for multi-gateway, hoping to take these two schemes as study cases to identify the common weaknesses of user authentication schemes. We show that they both are vulnerable to offline-dictionary attack, insider attack and fail to achieve forward secrecy and user anonymity. Thus, we propose an enhanced scheme. We prove that it achieves mutual authentication, provides secure session key agreement and can resist to known attacks.

Our research group has devoted a lot of efforts in user authentication scheme (see the homepage http://wangdingg.weebly.com/). We have published over 50 papers in respectable journals and conferences, such as IEEE TDSC, IEEE TIFS and ACM CCS, Usenix Security and NDSS.