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

房卫东[1,2],张武雄[1,2],杨 旸[1,2],张传雷[3],陈 伟[4]

(1. 中国科学院上海微系统与信息技术研究所无线传感网与通信重点实验室,上海 200051;2. 上海无线通信研究中心,上海 201210;
3. 天津科技大学计算机科学与信息工程学院,天津 300222; 4. 中国矿业大学计算机科学与技术学院,江苏徐州 221116)

摘 要: 为满足高安全级别场景(如军事、国家安全、银行等)的应用需求,进一步提高无线传感器网络用户认证协议的安全性,提出了基于生物特征识别的三因素用户认证协议.针对Althobaiti协议无法防御节点妥协攻击、模拟攻击、中间人攻击和内部特权攻击的安全缺陷,增加智能卡和密码作为协议基本安全因素,并利用生物特征标识信息生成函数与回复函数处理的生物特征标识作为附加安全因素;在密钥管理中,为每个节点配置了与网关节点共享唯一密钥,保证认证过程的独立性与安全性;实现用户自主选择与网关节点的共享密钥,提高公共信道通信的安全性;在网关节点不参与的情况下,设计密码和生物特征标识更新机制,保证二者的新鲜性.通过Dolev-Yao拓展威胁模型的分析与AVISPA的OFMC分析终端的仿真,结果证明该认证协议克服了Althobaiti协议安全缺陷,且对计算能力的需求小于公钥加密.权衡安全性与计算成本,该协议适用于资源受限且安全需求高的无线传感器网络应用.

关键词: 无线传感器网络; 信息安全; 三因素; 用户认证协议; 生物特征标识

中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2018) 03-0702-12

电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.03.028

BTh-UAP:Biometric-Based Three-Factor User Authentication Protocol for Wireless Sensor Network

FANG Wei-dong[1,2],ZHANG Wu-xiong[1,2],YANG Yang[1,2],ZHANG Chuan-lei[3],CHEN Wei[4]

(1. *Key Laboratory of Wireless Sensor Network & Communication,Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences,Shanghai* 200051,*China*; 2. *Shanghai Research Center for Wireless Communication,Shanghai* 201210,*China*;
3. *College of Computer Science and Information Engineering,Tianjin University of Science and Technology,Tianjin* 300222,*China*;
4. *School of Computer Science and Technology,China University of Mining and Technology,Xuzhou,Jiangsu* 221116,*China*)

Abstract: To meet the application requirements in high-level security scenarios (i.e.,military,national security and banks),and further enhance the security for user authentication protocol in wireless sensor network (WSN),the biometric-based three-factor user authentication protocol (BTh-UAP) is proposed. For defending against the node compromise attack, the simulated attack,the man-in-the-middle attack and the privileged-insider attack in Althobaiti protocol,the smart card and password are taken as its basic secure factors,and the biometric identification that is operated by the biometric identification information generation and reply function is introduced as additional secure factor. In key management,a unique shared key for each node combined with gateway node is delivered to guarantee the independence and security in authentication phase. The shared key between user and gateway node is autonomously chosen to improve the security of the common communication channel. Furthermore,in the circumstance for non-participation of node,the updating scheme for password and biometric identification is designed to achieve the freshness. The results demonstrate that BTh-UAP not only overcomes Althobaiti's security flaws,but also its requirements for computing capability are less than the public-key encryption via using the Dolev-Yao threat model analysis and AVISPA's OFMC simulation. The tradeoff between security and computing costs indicates

收稿日期:2016-03-21;修回日期:2017-05-10;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61471346,No. 61461136003);上海市自然科学基金(No. 17ZR1429100);上海市科技创新行动计划(No. 17511105903,No. 17DZ1200302);国家自然科学基金委员会-山西省人民政府煤基低碳联合基金(No. U1510115);青海省自然科学基金(No. 2016-ZJ-922Q);青蓝工程资助;中国博士后科学基金特别资助项目(No. 2013T60574);CEMEE国家实验室开放课题基金(No. CEMEE2017K0303B)

that BTh-UAP can be applied in high-level security scenarios for resource-constrained wireless sensor network.

Key words: wireless sensor network (WSN); information security; three-factors; user authentication protocol; biometric

1 引言

无线传感器网络(Wireless Sensor Network,WSN)作为传感器技术、微机电系统(Micro-Electro-Mechanical System,MEMS),通信技术、网络技术的融合,已广泛应用到许多领域[1].与此同时,用户终端的类型也越来越丰富,如笔记本电脑、手机、iPAD、各种手持终端设备等.在WSN应用中,用户查询节点感知信息通常有两种方式:一种是用户通过WSN基站或网关节点,发送查询指令,然后获取对应节点传回信息的方式,其安全性由WSN自身的安全策略予以保证,但时延较大,适用于信息轮询模式或信息上传周期较长的应用;另一种是用户不通过WSN基站或网关节点,直接从传感器节点获得实时数据,该方式具有较高的实时性,适用于各种实时应用,但在此方式中,用户合法性的验证就变得尤其重要.若一旦被非法用户接入,不仅会泄露传感器节点数据,还会使整个WSN面临巨大的安全威胁[2].

目前,加密技术[3]、安全路由协议[4]、节点信任管理[5]、安全网络编码[6]等安全技术可以有效地提升WSN的安全性,但上述技术并不完全适用于改进用户认证协议的安全性.围绕着提高用户认证协议安全性,研究人员提出了许多有价值的安全机制与认证协议,如基于智能卡的强安全认证与密钥协商协议[7],RFID用户认证协议的不可跟踪性分析[8],以及基于无线传感器网关的动态用户认证协议改进机制[9]等,这些研究有效地促进了WSN用户认证协议安全性的提高.

提高认证安全性的主要方式之一是增加认证过程的"因素"种类,通常情况下,用户认证协议可分为双因素(基于智能卡和密码)用户认证协议以及在此基础上的三因素用户认证协议.WSN用户认证协议的设计需要满足以下原则:传感器节点的计算量要低;有足够的安全性,可以防御多种安全攻击;满足必要的安全需求;用户可以自由选择自己的登陆密码,在需要时可自由更改密码;协议内容必须是简洁正确的,没有冗余.

尽管双因素用户认证协议可以满足一定的用户认证需求,但是无法完全满足高安全级别场景(如军事、国家安全、博物馆、银行等)的应用需求.随着模式识别技术和生物技术的快速发展,生物特征标识(常见用户生物特征标识包括指纹、脸型、手型和掌纹等)越来越受到用户认证技术研究的关注,这是因为生物特征标识具有以下优点[10]:

(1)生物特征标识不会丢失或忘记;

(2)生物特征标识不易被复制;

(3)生物特征标识不易伪造或分配;

(4)生物特征标识不易被猜测;

(5)生物特征标识不易破坏其他的生物特征标识.

为了进一步提高认证协议的安全性,拓展WSN高安全级别应用,本文提出基于用户生物特征标识的三因素用户认证协议(Biometric-based Three-factor User Authentication Protocol,BTh-UAP).该协议在智能卡和密码作为协议基本安全因素基础上,引入生物特征标识作为附加安全因素;通过为每个节点配置与网关节点共享唯一密钥,保证认证过程的独立性与安全性;通过实现用户与网关节点共享密钥的自主选择,提高公共信道通信的安全性;设计密码和生物特征标识更新机制,保证密码与生物特征标识的新鲜性.

2 相关工作

本节综述针对WSN用户认证协议的主要安全攻击,以及与本文研究密切相关的基于生物特征标识的用户认证协议研究现状.

2.1 安全攻击

针对WSN用户认证协议安全,存在的安全攻击主要有[11,12]:

节点妥协攻击(node compromise attack). 由于WSN通常部署在敌对环境或开放式无人值守的区域,又因成本限制,节点没有配置物理保护装置.因此,传感器节点易被攻击者捕获并妥协,进而造成节点存储的秘密参数易泄露.

密码猜测攻击(password guessing attack). 密码是攻击者发动猜测攻击的首要目标.用户为方便记忆密码,通常选择一些熟悉数字如生日、电话号码等低熵信息作为登陆密码.因此攻击者可以从含该密码的密码池中成功猜测出用户密码.攻击者也可通过获取密码相关参数,利用这些参数与密码之间的关联性猜测用户密码.

网关节点旁路攻击(gateway node bypass attack). 在认证协议中网关节点通常扮演注册中心的角色,协议执行时,用户向网关节点发送登陆请求消息,网关节点基于登陆请求消息决定传感器节点是否需回应用户请求.若攻击者在没有网关节点参与的情况下,成功通过认证,则会触发网关节点旁路攻击,使得攻击者在无合法授权的情况下访问到网络数据.

中间人攻击(man-in-the-middle attack). 在通信双方不知情的情况下,攻击者可以读取并创建传输消息.

内部特权攻击(privileged-insider attack). 当系统

管理方误用或泄露用户密码及其他秘密参数,由此可能导致在同一系统或其他系统内触发其他安全攻击.

智能卡丢失攻击(smart card loss attack). 当用户智能卡丢失或被窃取时,攻击者可通过智能卡存储的秘密参数,成功猜测用户密码,并在智能卡中注入错误信息或更换错误密码. 若攻击者在线利用用户智能卡成功通过密码认证,则被视为合法用户登录系统. 攻击者也可利用智能卡秘密参数创建合法的登陆请求消息,在没有成功猜出用户密码的情况下模仿合法用户访问网络信息.

重放攻击(replay attack). 攻击者不断重放之前截获的传输消息,实现登陆系统或欺骗合法用户相信其是合法服务提供商.

拒绝服务攻击(denial-of-service attack). 任何能引起合法用户拒绝提供服务的恶意或错误的行为称为拒绝服务攻击. WSN 存在多种触发拒绝服务攻击的途径. 若攻击者可以删除或操纵存储在系统数据库中的用户相关参数,而密码更换涉及参数的变化,故协议密码更换阶段易遭受拒绝服务攻击. 由于密码更新机制存在缺陷,攻击者可以更新替换错误的智能卡验证消息,致使合法用户无法成功登陆系统. 攻击者也可向全网以泛洪方式传播错误消息,导致合法用户的请求消息不能成功到达请求服务器,阻止合法用户访问网络数据. 由此可见,拒绝服务攻击可以阻止或抑制服务的正常执行.

相同身份多重用户登陆攻击(many logged-in users with the same login-ID attack). 不同的用户利用相同的身份标识登录网络,获取其他用户的数据.

验证-窃取攻击(stolen verifier attack). 由于某些与用户相关的数据存储在系统数据库或验证表中,为了在智能卡丢失或被窃取时及时撤销智能卡,禁止合法的恶意用户访问网络特权资源,系统需维持某个数据库或验证表. 发生验证-窃取攻击时,攻击者窃取网关节点或传感器节点维持的数据库或验证表,假装是协议合法参与实体,从而触发模拟攻击.

目前针对用户认证协议安全性的分析,主要是根据认证协议对上述攻击的防御情况展开的,同时,结合用户匿名性的实现,会话密钥安全与三因素安全的保证作为安全性能的提升.

2.2 研究现状

随着模式识别技术和生物技术的快速发展,近年来研究人员已提出多种基于生物特征标识的 WSN 用户认证协议及三因素用户认证协议,本小节主要侧重于指出其安全性缺陷,同时,简要概述近期 WSN 密码(口令)认证的研究现状.

Lee 等人[13]提出一种基于指纹的远距离智能卡用户认证协议,但该认证协议不能防御模拟攻击. Li 等人[14]提出了一种基于生物特征密钥的远程用户认证机制,该机制利用生物特征标识验证合法用户的正确性,但不能有效防御拒绝服务攻击. Yuan 等人[15]提出了一种基于生物特征标识的 WSN 三因素用户认证协议,然而该协议无法保证交换消息的完整性、不能防御节点妥协攻击和拒绝服务攻击. Lee 等人[16]证明 Li 协议存在安全漏洞,提出了一种改进的三因素用户认证协议,然而该协议不能防御重放攻击、也不能实现用户匿名性. Yoon 等人[17]针对 Yuan 协议存在的漏洞提出了一种基于生物特征标识的用户认证协议,但其没有利用密码因素,尽管改进了 Yuan 协议,但其依然存在安全缺陷,如传感器节点与用户间没有建立会话密钥、没有考虑传输消息的机密性、不能防御拒绝服务攻击等. Das[18]提出了一种双因素用户认证协议,宣称能抵御多种安全威胁,如相同身份多重用户攻击、密码猜测攻击、模拟攻击、重放攻击和验证-窃取攻击. Sekhar 等人[19]发现 Das 协议存在安全漏洞,不能防御用户模拟攻击、重放攻击和网关节点旁路攻击,因此提出了一种改进的三因素用户认证协议. An[20]证明 Das 协议存在安全漏洞,即不能防御密码猜测攻击、用户模拟攻击、服务器伪造攻击和内部攻击,其提出了一种改进的基于生物特征标识的远程用户认证协议,并宣称其提出的认证协议的安全性高于相关认证协议. Chaturvedi[21]等人针对 Li 协议和 An 协议存在的安全漏洞提出了一种改进的可建立会话密钥的三因素远程用户认证协议. Althobaiti 等人[22]提出了一种基于生物标识的 WSN 用户认证协议,该协议利用了用户生物特征标识作为协议安全基础,降低了计算复杂度,并有效地改善了用户认证协议的安全性,适用于节点资源受限的 WSN. 经研究发现该协议不能完全防御节点妥协攻击、GWN 模拟攻击、中间人攻击和内部特权攻击,其具体的安全性分析过程详见本文第 4 节“Althobaiti 协议及安全分析”.

密码(口令)因其使用简单,成本低廉,易更新等特点,故成为是应用较为广泛的身份认证方法之一. Liu 等人[23]提出了基于指纹的一次性密码用户认证协议. Kiani 与 Dalkilic[24]提出一种用于 WSN 动态认证的密码更新增强机制,该机制可以有效地抵抗重放和伪造攻击,减少用户密码泄漏风险. Liu 等人[25]提出一种基于动态密码的 WSN 用户认证协议,该协议使用了单向哈希函数与异或操作,具有较低的计算量与一定的安全性. 喻丽春[26]提出一种基于高级加密标准算法和公钥加密算法的一次性口令认证方案,提高了 WiFi 共享系统身份认证协议在的安全性. 韩伟力等人[27]提出了基于样本的模拟口令集生成算法,提高了真实口令覆盖率. 此外,王平等人[28]对口令安全研究现状进行了综述,总结了近 30 年来提出的几

个主流口令猜测算法,回顾了口令策略强度评价标准,对比了几个主流的口令强度评价器,并指出当前口令安全的研究整体尚处于起步阶段.

从上面的分析可以看出,WSN 用户认证协议的设计与安全性的提升,是一个不断分析、发现既有用户认证协议安全缺陷,并加以改进的过程. 本文后续将选用较为典型的 Althobaiti 用户认证协议作为研究基础,分析并指出其具体安全缺陷,提出具有较高安全性的 BTh-UAP 用户认证协议.

3　基础知识

为便于后续的分析与推导,本节将依据需要给出必要的攻击者威胁模型及攻击者的假定能力,同时,给出推导过程中所需的公式符号与意义.

3.1　假设与约定

由于 WSN 多部署在无人值守的开放式无线通信环境中,其安全性与传统有线网络相比更易受到安全威胁. 本文后续的安全性分析,将参考 Dolev 和 Yao 提出的在非安全开放式通信中的攻击者威胁模型(Dolev-Yao 模型).

其中,Dolev-Yao 模型对攻击者能力假设如下[29]:

(1)攻击者可获得所有经公共信道传输的消息;

(2)攻击者可冒充其他通信实体向用户发送消息;

(3)攻击者不能获得正确的随机数;

(4)攻击者没有正确的密钥就不能解密消息;

(5)攻击者不能破坏加密算法.

结合 WSN 用户认证协议特性,在分析用户认证协议安全性时,将补充参考 Kim[30] 提出的拓展 Dolev-Yao 攻击者模型,该模型中对攻击者能力假设如下:

(1)攻击者可妥协传感器节点,窃取存储的秘密参数;

(2)攻击者一旦获得用户的智能卡,可以获得卡中存储的参数信息;

(3)为方便记忆,通常用户身份标识和密码是低熵的;

(4)网关节点是诚实的;

(5)传感器节点没有配置防篡改装置.

3.2　符号与意义

本文后续协议分析与推导过程中使用的公式符号与意义见表 1.

表 1　符号及其意义

符号:意义	符号:意义
U_i:标识号为 i 的用户;	$E_k(\cdot)$:对称加密函数;
ID_i:U_i 身份标识;	$D_k(\cdot)$:对称解密函数;
B_i:U_i 生物特征标识;	$h(\cdot)$:哈希函数;
PW_i:U_i 密码;	GWN:网关节点;
MK_{SN_j}:SN_j 与 GWN 的共享密钥;	σ_i:生物特征标识密钥;
SN_j:标识号为 j 的传感器节点;	τ_i:生物特征标识公共参数;
ID_{SN_j}:SN_j 身份标识;	T:时间戳;
X:GWN 与部署传感器节点的共享秘密参数;	ΔT:允许最大传输延迟;
Gen $(\cdot)$:生物特征标识信息生成函数;	$\oplus$:比特异或操作;
Rep $(\cdot)$:生物特征标识信息回复函数;	$\|$:比特级联操作.

4　Althobaiti 协议及安全分析

4.1　Althobaiti 协议描述

Althobaiti 协议以生物特征标识作为协议安全基础,由三个阶段组成,具体包括:注册阶段、登陆阶段和认证阶段.

(1)注册阶段

当新用户 U_i 需要访问传感器网络数据时,向 GWN 注册,U_i 和 GWN 行下列操作:

(a)系统随机选择密钥 ek_i,置于 GWN 内存中,作为 GWN 与 U_i 的共享密钥;

(b)U_i 输入身份标识 ID_i 和生物特征密钥 B_i,计算 $h(B_i)$、$BE=h(B_i)\oplus ek_i$,在 U_i 中存储 BE;

(c)GWN 计算 $F_i=h(ID_i\oplus X)$,经安全信道向 U_i 发送注册消息$\{ID_i,F_i\}$;

(d)U_i 存储参数$\{ID_i,F_i,h(ek_i),BE\}$.

(2)登陆阶段

U_i 完成注册,登陆 WSN 时执行下列操作:

(a)U_i 输入身份标识 ID_i 和生物特征密钥 B_i,计算:$N=h(B_i)$、$ek_i'=BE\oplus h(B_i)$;

(b)U_i 计算 $h(ek_i')$,验证 $h(ek_i')=h(ek_i)$ 是否成立,若成立则向 GWN 发送登陆请求消息$\{ID_i,\text{request}\}$,否则,终止操作.

(3)认证阶段

实现 U_i 和 SN_j 的双向认证,建立会话密钥,执行下列操作:

(a)GWN 收到$\{ID_i,\text{request}\}$后,向 U_i 发送认证请求$\{R\}$作为登陆回应,其中 R 表示随机挑选. U_i 收到$\{R\}$后,利用加密密钥 ek_i 加密$\{R,T_1\}\rightarrow E_{ek_i}\{R,T_1\}$,其中 T_1 表示 U_i 当前时间戳,经公共信道向 GWN 发送认证请求消息 $E_{ek_i}\{R,T_1\}$;

(b)GWN 在时刻 T_2 接收 $E_{ek_i}\{R,T_1\}$,利用 ek_i 解密 $D_{ek_i}\{R,T_1\}$,验证$|T_1-T_2|\leqslant\Delta T$ 是否成立,若不成立则终止操作,否则,传感器节点 SN_j 回应 U_i 请求.

(c)GWN 计算:

$$Y_i=MAC_{F_i}(ID_i\|ID_{SN_j}\|T_3)$$

$$F_i=h(ID_i\oplus X)$$

其中,T_3 表示 GWN 当前时间戳. GWN 经公共信道向 SN_j 发送消息$\{ID_i,Y_i,T_3\}$;

(d)SN_j 在时刻 T_4 接收$\{ID_i,Y_i,T_3\}$,首先验证$|T_4-T_3|\leqslant\Delta T$ 是否成立,若不成立则终止操作,否则,计算:

$$Y_i'=MAC_{F_i}(ID_i\|ID_{SN_j}\|T_3)$$

$$F_i=h(ID_i\oplus X)$$

验证 $Y_i'=Y_i$ 是否成立,若不成立则终止操作,否

则,SN_j 以 RM 回应用户请求,计算:

$$V_i = h(ID_i \| F_i \| T_5)$$
$$C_i = h(RM)$$
$$L = E_{V_i}(RM, C_i)$$

经公共信道向 U_i 发送$\{L, T_5\}$,其中 T_5 表示 SN_j 当前时间戳;

(e)U_i 在时刻 T_6 接收$\{L, T_5\}$,首先认证$|T_6 - T_5| \leqslant \Delta T$ 是否成立,若不成立则终止操作,否则,计算:

$$V_i = h(ID_i \| F_i \| T_5)$$
$$D_{V_i}(L) = (RM', C_i')$$
$$C_i^* = h(RM')$$

若 $C_i^* = C_i'$,则 U_i 接受 RM 作为合法请求回应,否则,U_i 拒绝 RM,其中 $V_i = h(ID_i \| F_i \| T_5)$被认为是 U_i 和 SN_j 的会话密钥.

4.2 安全性分析

Althobaiti 协议是作为典型的基于生物特征标识用户认证协议,利用哈希函数、异或操作、级联操作和对称加密,未使用复杂的非对称加密,有效地降低计算量,可以防御智能卡丢失攻击、验证-窃取等多种安全攻击,但 Althobaiti 协议安全仅基于生物特征值标识,存在一定的局限性. 本文基于 Dolev-Yao 攻击者拓展模型,分析发现 Althobaiti 协议存在下列安全缺陷:

(1)节点妥协攻击

假设攻击者 A 妥协登陆传感器节点 SN_j,获取秘密参数 X,在认证阶段截获消息$\{ID_i, Y_i, T_3\}$和$\{L, T_5\}$,A 计算:

$$F_i = h(ID_i \oplus X)$$
$$V_i = h(ID_i \| F_i \| T_5)$$

其中,V_i 作为 SN_j 与的会话密钥. 因此,A 可能得到会话密钥 V_i. 此外 A 通过以下步骤可以获得妥协 U_i 与其他非妥协节点 SN_j'间的会话密钥.

(a)GWN 在认证阶段向 SN_j'发送消息$\{ID_i, Y_i', T_3'\}$和消息$\{L', T_5'\}$,其中,

$$F_i = h(ID_i \oplus X)$$
$$Y_i' = \mathrm{MAC}_{F_i}(ID_i \| SN_j' \| T_3')$$
$$C_i' = h(RM)$$
$$V_i' = h(ID_i \| F_i \| T_5')$$
$$L' = E_{V_i'}(RM, C_i').$$

(b)A 截获消息$\{ID_i, Y_i', T_3'\}$和$\{L', T_5'\}$,得到参数 X、ID_i 和 T_5',计算:$V_i' = h(ID_i \| F_i \| T_5')$,则 A 能获得 U_i 与 SN_j'间的会话密钥. 当 A 成功妥协一个登陆节点后,可以获得 U_i 与 SN_j'间所有会话密钥,因而该认证协议不能防御节点妥协攻击.

(2)GWN 模拟攻击

攻击者 A 通过以下过程可以成功触发 GWN 模拟攻击:

(a)A 物理妥协传感器节点 SN_j,获取秘密参数 X,在认证阶段截获消息$\{ID_i, Y_i, T_3\}$.

(b)A 计算:

$$F_i' = h(ID_i \oplus X)$$
$$Y_i' = MAC_{F_i'}(ID_i \| SN_j' \| T_3')$$

其中,SN_j'表示 U_i 查询节点、T_3'表示 A 当前时间戳,经公共信道向 SN_j'发送消息$\{ID_i, Y_i', T_3'\}$.

(c)SN_j'收到$\{ID_i, Y_i', T_3'\}$后,首先验证 T_3'的新鲜性,若不合法则终止操作,否则,计算:

$$F_i = h(ID_i \oplus X)$$
$$Y_i^* = MAC_{F_i'}(ID_i \| SN_j' \| T_3')$$

验证 $Y_i^* = Y_i'$是否成立. 若成立,SN_j'以 RM'回应用户查询请求,计算:

$$V_i' = h(ID_i \| F_i \| T_5')$$
$$C_i' = h(RM')$$
$$L' = E_{V_i'}(RM', C_i')$$

其中,T'表示 SN_j'当前时间戳,经公共信道向 U_i 发送消息$\{L', T_5'\}$.

由于 A 能利用参数 X、ID_i 和 T_5',计算出会话密钥 V_i',因而,该协议不能防御 GWN 模拟攻击.

(3)中间人攻击

攻击者 A 通过以下过程触发中间人攻击:

(a)A 物理妥协传感器节点 SN_j,获取秘密参数 X,在认证阶段截获消息$\{ID_i, Y_i, T_3\}$.

(b)A 计算:

$$F_i^* = h(ID_i \oplus X)$$
$$Y_i^* = MAC_{F_i^*}(ID_i \| SN_j \| T_3^*)$$

其中,T_3^* 表示 A 当前时间戳,经公共信道向 SN_j 更改消息$\{ID_i, Y_i^*, T_3^*\}$.

(c)SN_j 收到$\{ID_i, Y_i^*, T_3^*\}$后,首先验证 T_3^* 的新鲜性,若新鲜,则计算:

$$F_i = h(ID_i \oplus X)$$
$$Y_i^{**} = MAC_{F_i}(ID_i \| SN_j \| T_3^*)$$

验证 $Y_i^* = Y_i^{**}$ 是否成立,若成立,SN_j 以 RM^* 回应用户请求,计算:

$$V_i^* = h(ID_i \| F_i \| T_5^*)$$
$$C_i^* = h(RM^*)$$
$$L^* = E_{V_i^*}(RM^*, C_i^*)$$

向 U_i 发送$\{L^*, T_5^*\}$;

(d)A 截获消息$\{L^*, T_5^*\}$,计算,

$$V_i^{**} = h(ID_i \| F_i^* \| T_5^*)$$

解密 L^* 获取参数 RM^*、C^*. 此外,攻击者 A 可以创建回应 RM^{**} 替换 RM^*,计算:

$$C_i^{**} = h(RM^{**})$$
$$L^{**} = E_{V_i^{**}}(RM^{**}, C_i^{**})$$

最终,A 向 U_i 发送$\{L^{**}, T_5^*\}$. U_i 会成功认证$\{L^{**}, T_5^*\}$,U_i 将 RM^{**}作为请求合法回应,因此该协议不能防御中间人攻击.

(4)内部特权攻击

在注册阶段,GWN 随机生成注册 U_i 加密密钥 ek_i,而 ek_i 存储在,GWN 数据库中. ek_i 用来加密随机挑战 R 和 T_1. 因此,GWN 内部攻击者可以轻易获取 ek_i 伪造 U_i,因此该协议不能防御内部特权攻击.

5　基于生物特征标识的三因素用户认证协议(BTh-UAP)

从4.2 节的分析可看出,Althobaiti 认证协议存在无法防御节点妥协攻击、GWN 模拟攻击、中间人攻击和内部特权攻击的安全缺陷. 为改进这些安全缺陷,本文引入生物特征标识的同时,结合智能卡和密码,提出轻量级 WSN 的三因素用户认证协议(BTh-UAP),从以下方面进行改进:

(1)增加智能卡和密码做为协议基本安全因素;

(2)利用 Gen(·)和 Rep(·)函数处理生物特征标识;

(3)为每个节点配置与 GWN 唯一共享密钥 MK_{SN_j};

(4)由 U_i 选择与 GWN 的共享唯一密钥;

(5)引入密码和生物特征标识更新机制,在 GWN 不参与的情况下,U_i 可自主更换密码和生物特征标识.

BTh-UAP 协议由注册阶段、登陆阶段、认证阶段、密码和生物特征标识更改阶段组成.

5.1　注册阶段

当 U_i 访问传感器网络时,需向 GWN 注册,其注册流程如图 1 所示.

(1)U_i 选择身份标识 ID_i 和密码 PW_i,输入生物特征标识 B_i,生成随机数 K,利用生物特征标识信息生成函数 Gen(·)生成 B_i 对应的密钥 σ_i 和公共参数 τ_i,即Gen$(B_i)=(\sigma_i,\tau_i)$,其中 σ_i 仅为 U_i 所知;

(2)U_i 计算:$RPW_i=h(PW_i\|K)$,选择与 GWN 的共享密钥 key_i,通过安全信道向 GWN 发送注册请求消息$\langle RPW_i, ID_i, key_i\rangle$;

(3)GWN 收到来自 U_i 的注册请求后,在其数据库中存储 key_i、生成随机数 K_{GWN},计算:

$$r_i=h(ID_i\|X_{\mathrm{GWN}})$$

生成含参数$\{r_i, h(\cdot)\}$的智能卡 SC_i,通过安全信道发送至 U_i;

(4)收到 GWN 生成的 SC_i 后,U_i 计算,

$$e_i=h(ID_i\|\sigma_i)\oplus K$$
$$f_i=h(ID_i\|RPW_i\|\sigma_i)$$
$$g_i=h(ID_i\|\sigma_i)\oplus key_i$$
$$l_i=r_i\oplus h(ID_i\|K)=h(ID_i\|X_{\mathrm{GWN}})\oplus h(ID_i\|K)$$

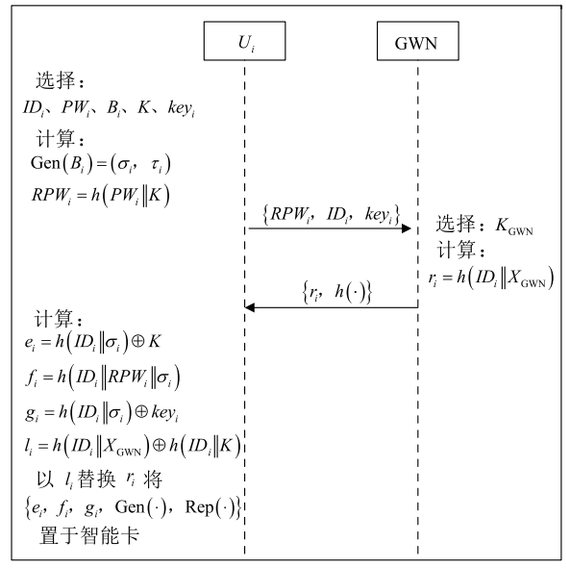

图1　注册阶段

利用 l_i 替换 SC_i 中原有的 r_i,并存储参数$\{e_i, f_i, g_i, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), \tau_i\}$.

5.2　登陆阶段

注册阶段完成后,U_i 登陆传感器网络,其登陆过程如图 2 所示.

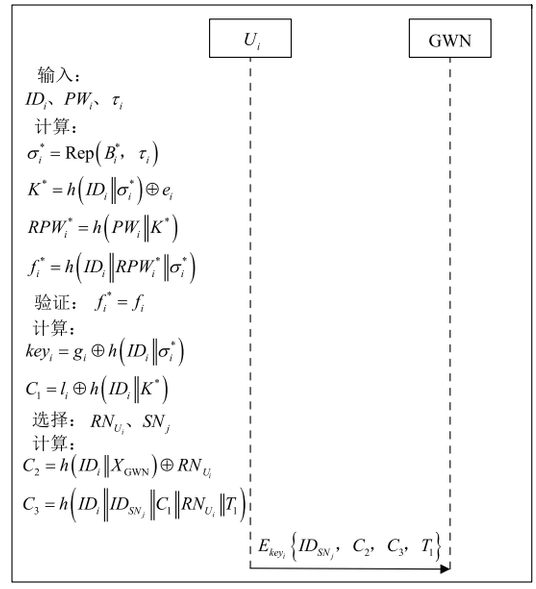

图2　登陆阶段

(1)U_i 把 SC_i 插入读卡装置中,输入 ID_i、PW_i 和生物特征标识 B_i^*;

(2)SC_i 计算:

$$\sigma_i^*=\mathrm{Rep}(B_i^*,\tau_i)$$
$$K^*=h(ID_i\|\sigma_i^*)\oplus e_i$$

$$RPW_i^* = h(PW_i \| K^*)$$

$$f_i^* = h(ID_i \| RPW_i^* \| \sigma_i^*)$$

验证 $f_i^* = f_i$ 是否成立,若不成立则终止操作,否则,继续下一步操作;

(3) SC_i 计算:

$$key_i = g_i \oplus h(ID_i \| \sigma_i')$$

$$C_1 = l_i \oplus h(ID_i \| K^*) = h(ID_i \| X_{GWN})$$;

(4) SC_i 生成随机数 RN_{U_i},选择需访问的节点 SN_j,计算:

$$C_2 = C_1 \oplus RN_{Ui} = h(ID_i \| X_{GWN} \oplus RN_{U_i}$$

$$C_3 = h(ID_i \| ID_{SN_j} \| C_1 \| RN_{U_i} \| T_1)$$

经公共信道向 GWN 发送登陆请求:

$$E_{key_i}(ID_{SN_j}, C_2, C_3, T_1)$$

其中,T_1 表示 SC_i 当前时间戳.

5.3 认证阶段

U_i 登陆传感器网络后,再访问 SN_j 数据前,GWN 和 SN_j 需验证 U_i 的合法性,同时,U_i 也需验证 SN_j 的合法性. 认证过程如图 3 所示.

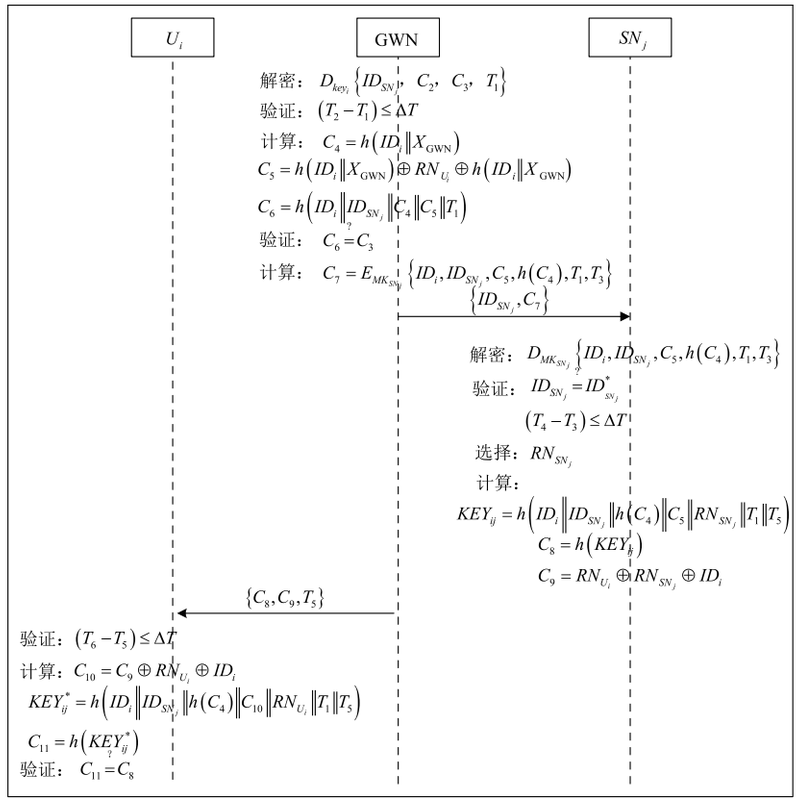

图3 认证阶段

(1) GWN 在 T_2 时刻收到来自用户登陆请求,利用 key_i 解密 $E_{key_i}(ID_{SN_j}, C_2, C_3, T_1)$,得到参数($ID_{SN_j}, C_2, C_3, T_1$)后,首先验证 $|T_2 - T_1| \le \Delta T$ 是否成立,若不成立则终止操作,否则,GWN 计算:

$$C_4 = h(ID_i \| X_{GWN})$$

$$C_5 = C_2 \oplus h(ID_i \| X_{GWN})$$

$$= h(ID_i \| X_{GWN} \oplus RN_{U_i} \oplus h(ID_i \| X_{GWN})$$

$$= RN_{U_i}$$

$$C_6 = h(ID_i \| ID_{SN_j} \| C_4 \| C_5 \| T_1)$$

验证 $C_6 = C_3$ 是否成立,若成立则 GWN 成功验证 U_i 是合法用户,否则,终止操作;

(2) GWN 利用 SN_j 的主密钥 MK_{SN_j},计算,

$$C_7 = E_{MK_{SN_j}}[ID_i, ID_{SN_j}, C_5, h(C_4), T_1, T_3]$$

其中,T_3 表示 GWN 当前时间戳,经公共信道向 SN_j 发送认证请求$\langle ID_{SN_j}, C_7 \rangle$;

(3) SN_j 在时刻 T_4 收到$\{ID_{SN_j}, C_7\}$,利用 MK_{SN_j}解密 C_7 得到参数 ID_i、$ID_{SN_j}^*$、C_5、$h(C_4)$、T_1 和 T_3,验证 $ID_{SN_j}^* = ID_{SN_j}$和 $|T_3 - T_4| \le \Delta T$ 是否成立,若上述两项均成立,则 SN_j 成功验证 U_i 的合法性,若存在不成立项则终止操作;

(4) SN_j 生成随机数 RN_{SN_j},计算其与 U_i 的会话密钥:

$$KEY_{ij} = h(ID_i \| ID_{SN_j} \| h(C_4) \| C_5 \| RN_{SN_j} | T_1 | T_5)$$

其中,T_5 为 SN_j 当前时间戳,计算,

$$C_8 = h(KEY_{ij})$$

$$C_9 = C_5 \oplus RN_{SN_j} \oplus ID_i = RN_{U_i} \oplus RN_{SN_j} \oplus ID_i$$

经公共信道向 U_i 发送认证回应消息$\langle C_8, C_9, T_5 \rangle$;

(5) U_i 在 T_6 时刻收到$\langle C_8, C_9, T_5\rangle$,首先验证$|T_5 - T_6| \leqslant \Delta T$ 是否成立,若不成立,则终止操作,否则,SC_i 计算:

$$C_{10} = C_9 \oplus RN_{U_i} \oplus ID_i = RN_{SNj}$$
$$KEY'_{ij} = h(ID_i \| ID_{SN_j} \| h(C_4) \| C_{10} \| RN_{U_i} \| T_1 \| T_5)$$
$$C_{11} = h(KEY'_{ij})$$

SC_i 验证 $C_{11} = C_8$ 是否成立,若成立,则 U_i 成功验证 SN_j 是合法节点,否则,终止操作. 其中 $KEY_{ij} = KEY'_{ij}$. SN_j 储存 KEY_{ij},U_i 储存 KEY'_{ij}作为通信的共享会话密钥.

5.4　密码和生物特征标识更新阶段

在密码和生物特征标识更新阶段,GWN 不参与执行操作. 本阶段可分为三个相对独立的过程.

(1)更新密码过程

本过程中,U_i 执行以下操作:

(a) U_i 把智能卡 SC_i 插入读卡装置,输入 ID_i、旧密码 PW_i^{old} 和生物特征标识 B_i,SC_i 计算:

$$\sigma_i = \mathrm{Rep}(B_i, \tau_i)$$
$$K = h(ID_i \| \sigma_i) \oplus e_i$$
$$RPW_i^{old} = h(PW_i^{old} \| K)$$
$$f_i^{old} = h(ID_i \| RPW_i^{old} \| \sigma_i)$$

若满足 $f_i^{old} = f_i$,则输入新密码 PW_i^{new},否则,终止操作.

(b)输入新密码 PW_i^{new},SC_i 计算:

$$RPW_i^{new} = h(PW_i^{new} \| K)$$
$$f_i^{new} = h(ID_i \| RPW_i^{new} \| \sigma_i)$$

在 SC_i 中,用 f_i^{new} 替换 f_i.

(2)更新生物特征标识过程

本过程中,U_i 执行以下操作:

(a) U_i 把智能卡 SC_i 插入读卡装置,输入 ID_i、PW_i 和旧生物特征密钥 B_i^{old},SC_i 计算:

$$\sigma_i^{old} = \mathrm{Rep}(B_i^{old}, \tau_i)$$
$$K^* = h(ID_i \| \sigma_i^{old}) \oplus e_i$$
$$RPW_i = h(PW_i \| K^*)$$
$$f_i^{old} = h(ID_i \| RPW_i^{old} \| \sigma_i^{old})$$

若满足 $f_i^{old} = f_i$,则输入新的生物特征标识 B_i^{new},否则,终止操作,

(b) U_i 输入新的生物特征标识 B_i^{new},SC_i 计算:

$$(\sigma_i^{new}, \tau_i^{new}) = \mathrm{Gen}(B_i^{new})$$
$$e_i^{new} = h(ID_i \| \sigma_i^{new}) \oplus h(ID_i \| K^*)$$

在 SC_i 中,用 e_i^{new}、τ_i^{new} 分别替换 e_i、τ_i.

(3)密码和生物特征标识同时更新

本过程中,执行以下操作:

(a) U_i 把智能卡 SC_i 插入读卡装置,输入 ID_i、旧密码 PW_i^{old} 及旧生物特征标识 B_i^{old},SC_i 计算:

$$\sigma_i^{old} = \mathrm{Rep}(B_i^{old}, \tau_i)$$
$$K^* = h(ID_i \| \sigma_i^{old}) \oplus e_i$$
$$RPW_i^{old} = h(PW_i^{old} \| K^*)$$
$$f_i^{old} = h(ID_i \| RPW_i^{old} \| \sigma_i^{old})$$

若满足 $f_i^{old} = f_i$,则输入其选择的新密码 PW_i^{new} 和新生物标识 B_i^{new},否则,终止操作;

(b) U_i 输入新的密码 PW_i^{new} 和新生物特征标识 B_i^{new},SC_i 计算:

$$(\sigma_i^{new}, \tau_i^{new}) = \mathrm{Gen}(B_i^{new})$$
$$e_i^{new} = h(ID_i \| \sigma_i^{new}) \oplus h(ID_i \| K^*)$$
$$RPW_i^{new} = h(\| PW_i^{new} \| K^*)$$
$$f_i^{new} = h(ID_i \| RPW_i^{new} \| \sigma_i^{new})$$

在 SC_i 中,用 e_i^{new}、f_i^{new}、τ_i^{new} 分别替换 e_i、f_i、τ_i.

6　安全和性能分析

6.1　安全性分析

本小节将利用 Dolev-Yao 拓展威胁模型分析 BTh-UAP 协议,并与 Althobaiti 协议、Yuan 协议、Yoon 协议的安全性进行比较.

6.1.1　BTh-UAP 协议安全性分析

(1)节点妥协攻击

假设攻击者物理妥协传感器节点 SN_j,访问 SN_j 的即时数据. 因为传感器节点没有配置防篡改硬件,攻击者可以获取 SN_j 存储的机密信息包括节点主密钥和会话秘密. 由于会话密钥与 RN_{U_i}、U_i 和 SN_j 的时间戳有关,因此全网节点与用户间的会话密钥是有所差异的. 传感器网络部署之前,系统为每个节点预置一个唯一随机主密钥. 即使攻击者妥协 SN_j 的主密钥,但其他合法节点仍然可以和用户安全通信. 因此一个节点妥协不会泄露任何与其他节点和用户相关信息,所以可防御节点妥协攻击.

(2)密码猜测攻击

由于用户密码以 $RPW_i = h(PW_i \| K)$ 隐藏方式传输,攻击者在未获取随机数 K,且 $h(\cdot)$ 是单向函数的情况下,不可能成功猜测出用户密码,但若攻击者俘获了登陆节点 SN_j,则可以在一定程度上发起密码猜测攻击,在这种情况下,增大随机数 K 的取值范围,可以增大密码猜测的难度,所以可以减弱密码猜测攻击.

(3)GWN 模拟攻击

假设攻击者物理妥协登陆节点 SN_j,因 MK_{SN_j} 与 SN_j 一一对应,故参数 $K_j = h(ID_{SN_j} \oplus MK_{SN_j})$ 也与 SN_j 一一对应. 若攻击者截获消息$\{ID_i, Y_j\}$后,面对传感器节点SN'_j模拟 GWN,由于,

$$f_i^{**} = h(ID_{SN'_j} \| f_i^*)$$
$$Y'_j = E_{K'_j}\{D_i, ID'_{SN_j}, T_1', T_2'\}$$

攻击者不能创建合法的$\{ID_i, Y'_j\}$,所以可以防御 GWN

模拟攻击.

(4)中间人攻击

假设攻击者截获用户合法登陆请求 $E_{key_i}\{ID_{SN_j},C_2,C_3,T_1\}$,由于攻击者未获知密钥 key_i,因此攻击者不能解密登陆请求消息.另一方面,假设攻击者通过某种途径获知 key_i,由于更改 C_2、C_3,需知道 C_1,然而攻击者未获知 ID_i 和 X_{GWN},且因哈希函数的单向特性,在这种情况下,更改 C_2、C_3 是不可行的,所以可防御中间人攻击.

(5)内部特权攻击

在 BTh-UAP 注册阶段,内部特权攻击者试图从 GWN 上推导获得参数 PW_i 和 σ_i,发起 U_i 向 GWN 发送的注册请求消息 $\{ID_i,RPW_i,key_i\}$,其中 $RPW_i=h(PW_i\|K)$.因为内部特权攻击者未获知 K,依据哈希函数单向特性,理论上推导 PW_i 是不可行的.此外,假设合法用户 U_i 是恶意攻击者,可从智能卡中获得参数

$$\{e_i,f_i,g_i,r_i^*,\tau_i,\mathrm{Gen}(\cdot),\mathrm{Rep}(\cdot),t\}$$

计算:

$$e_i=\mathrm{Rep}(B_i,\tau_i)$$
$$K=h(ID_i\|\sigma_i)\oplus e_i$$
$$h(ID_i\|X_s)=r_i^*\oplus h(ID_i\|K)$$

然而 X_{GWN}不能从 $h(ID_i\|X_{GWN})$直接获取,其猜测的成功率$\frac{1}{2^k}$(其中,k 表示 X_{GWN}的比特数),由于$\frac{1}{2^k}$值很小,可以忽略不计,所以可以防御内部特权攻击.

(6)智能卡丢失攻击

假设合法用户 U_i 的智能卡 SC_i 丢失或被窃取,攻击者可以从 SC_i 获得 e_i、f_i 和 r_i^*,其中,

$$e_i=h(ID_i\|\sigma_i)\oplus K$$
$$f_i=h(ID_i\|RPW_i\|\sigma_i)$$
$$r_i^*=r_i\oplus Kh(ID_i\|X_s)\oplus h(ID_i\|K)$$

K 表示只为 U_i 所知的随机数.因为智能卡没有防篡改机制,攻击者在未获知 ID_i、K、PW_i、σ_i 的条件下,依据哈希函数 $h(\cdot)$的单向性,理论上计算 U_i 的 PW_i 和 σ_i 是不可行的,同理,理论上计算 GWN 的 X_{GWN}也是不可行的,所以可以防御智能卡丢失攻击.

(7)重放攻击

攻击者发送合法 U_i 之前发送过的消息阻碍 GWN 消息的正常接收.假设攻击者截获登陆请求 $E_{key_i}\{ID_{SN_j},C_2,C_3,T\}$,若攻击者向 GWN 重放截获的登陆请求消息 $E_{key_i}\{ID_{SN_j},C_2,C_3,T\}$,但无法通过时间戳认证,所以可以防御重放攻击.

(8)拒绝服务攻击

GWN 向 SN_j 发送认证请求消息 $\{ID_{SN_j},C_7\}$,SN_j 向 U_i 发送认证回应消息 $\{C_8,C_9,T_5\}$.若攻击者阻碍 $\{ID_{SN_j},C_7\}$到达 SN_j,$\{C_8,C_9,T_5\}$到达 U_i,则 SN_j 和 U_i 均知道存在控制消息的恶意丢弃.另一方面,若攻击者通过恶意泛洪的方式使登陆请求到达 SN_j,其需进行一次加密操作和两次哈希操作,因为加密操作和哈希操作的单向有效性,检查恶意请求的合法性不需太多能量、内存和计算能力,所以可以防御拒绝服务攻击.

(9)相同身份多重用户登录攻击

用户隐藏密码哈希值与 PW_i、K 和 σ_i 有关.即使用户 U_i 和 U_j 有相同的密码 PW,$f_i=h(ID_i\|RPW_i\|\sigma_i)$和 $f_j=h(ID_j\|RPW_j\|\sigma_j)$也存在差异,其中,$\mathrm{Gen}(B_i)=(\sigma_i,\tau_i)$、$\mathrm{Gen}(B_j)=(\sigma_j,\tau_j)$,$ID_i$ 和 ID_j 分别表示 U_i 和 U_j 的身份标识,B_i 和 B_j 分别表示 U_i 和 U_j 的生物特征标识.这样即使 U_i 和 U_j 有相同的密码 PW,登陆网络之前,必须通过生物特征标识验证,所以可以防御相同身份多重用户登录攻击.

(10)验证-窃取攻击

用户认证协议本身不存储任何用于验证的验证器或密码表,因此网络内部攻击者无法窃取用户的密码和生物特征标识,同时,GWN 和 U_j 不用维持验证器或密码表用于用户登陆请求的验证,所以可以防御验证-窃取攻击.

(11)用户匿名

假设攻击者在登陆阶段截获登陆请求 $E_{key_i}\{ID_{SN_j},C_2,C_3,T_1\}$,在认证阶段截获认证请求 $\{ID_{SN_j},C_7\}$和认证回应 $\{C_8,C_9,T_5\}$,这些参数由哈希函数、随机数 RN_{U_i}、RN_{SN_j}和时间戳 T_1、T_5 决定.因此每一轮运行消息是不同的,攻击者不能成功链接 U_i 两条登陆消息,所以可实现用户匿名性.

(12)会话密钥安全

假设攻击者在登陆阶段截获了登陆请求 $E_{key_i}\{ID_{SN_j},C_2,C_3,T_1\}$,在认证阶段和密钥建立阶段截获了认证请求 $\{ID_{SN_j},C_7\}$和认证回应 $\{C_8,C_9,T_5\}$.其中,会话密钥为,

$$C_4=h(ID_i\|X_s)$$
$$KEY_{ij}=h(ID_i\|ID_{SN_j}\|h(C_4)\|C_5\|RN_{SN_j}\|T_1\|T_5)$$

为计算 KEY_{ij},攻击者需知道 ID_i、X_s、RN_{U_i}和 RN_{SN_j},依据哈希函数的单向性,攻击者计算 KEY_{ij}是不可行的,所以会话密钥是安全的.

(13)三因素安全

在三因素安全模型中,攻击者至少了解三因素其中的两个因素才能发动模拟攻击,获取第三个因素或妥协用户的匿名性.本文提出的 BTh-UAP 协议可以保护用户的匿名性,即使用户的智能卡丢失或泄露,攻击者也无法获取 ID_i、X_{GWN}、PW_i 和 σ_i.依据哈希函数的单向性,攻击者不能更改登陆请求和认证请求或回应消息,因此,本文提出的 BTh-UAP 认证协议可以满足三因素安全特性.

由上面的分析可见,BTh-UAP 协议除了能防御上

述安全攻击,还能实现用户匿名、保证会话密钥安全和三因素安全.

6.1.2 安全性比较

结合 2.1 节提出的安全攻击,BTh-UAP 与 Althobaiti 协议、Yuan 协议、Yoon 协议的安全性能比较结果如表 2 所示,其中,"√"表示可以抵御该种攻击,"×"表示无法抵御该种攻击.

表 2　安全攻击比较

安全特性	Althobaiti 协议	Yuan 协议	Yoon 协议	BTh-UAP 协议
节点妥协攻击	×	×	√	√
密码猜测攻击	√	√	√	√
GWN 模拟攻击	×	√	√	√
中间人攻击	×	√	√	√
内部特权攻击	×	√	×	√
智能卡丢失攻击	√	√	√	√
重放攻击	√	√	√	√
拒绝服务攻击	√	×	×	√
相同身份多重用户登录攻击	√	√	√	√
验证窃取攻击	√	√	√	√

6.2 形式化分析

将本文提出三因素用户认证协议(BTh-UAP)转换为 HLPSL 语言,利用 AVISPA[31] 的 OFMC 分析终端进行仿真,结果如图 4 所示.

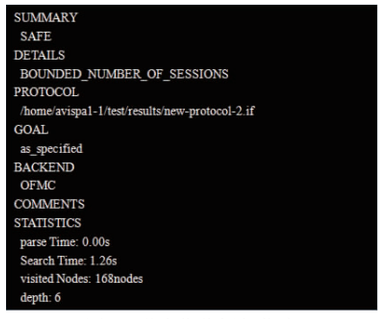

图4　形式化分析与仿真

从仿真结果得知,本文提出 BTh-UAP 三因素协议在 OFMC 后端运行了 1.26s,访问了 168 个节点,没有出现重复攻击、中间人和被动攻击轨迹,因此可以防御重放攻击、中间人攻击和内部特权攻击.

6.3 性能分析

Althobaiti 协议与 BTh-UAP 协议各阶段参与实体的计算成本比较结果如表 3 所示,其中,T_h 表示哈希操作、T_X 表示异或操作、T_{Gen}表示 Gen 操作、T_{Rep}表示 Rep 操作、T_{MAC}表示 MAC 操作、T_E 表示对称加密、T_D 表示对称解密.

从表 3 可以看出,Bth-UAP 认证协议增加了 Gen 操作和 Rep 操作,未使用复杂的非对称加密操作,减少了 MAC 操作. 尽管 Bth-UAP 三因素认证协议的总计算量高于 Althobaiti 协议、Yuan 协议和 Yoon 协议,但增加部分主要由 U_i 和 GWN 承担,U_i 和 GWN 计算能力远高于 SN_j,而传感器节点 SN_j 只在认证阶段进行 $T_D+3T_h+2T_X$ 运算,增加两次异或操作,减少了 MAC 操作,不涉及复杂的对称加密,有效地降低了传感器节点的计算复杂度,减少了节点的能量消耗. 权衡安全性与计算成本,本文提出的三因素认证协议适用于安全级别需求高的 WSN 应用.

表 3　计算开销比较

阶段		注册阶段	登陆阶段	认证阶段	密码和生物标识更新阶
Althobaiti 协议	U_i	T_h+T_X	$2T_h+T_X$	$T_E+T_h+T_D$	–
	GWN	T_h	–	$T_h+T_D+T_{\text{MAC}}$	–
	SN_j	–	–	$3T_h+T_{\text{MAC}}+T_E$	–
Yuan 协议	U_i	$2T_h$	$4T_h+T_X$	T_h+T_X	所有计算
	GWN	$2T_h+T_X$	$4T_h+2T_X$	$3T_h+T_X$	–
	SN_j	–	–	T_h+T_X	–
Yoon 协议	U_i	T_h	$2T_h+2T_X$	T_h	–
	GWN	$2T_h+2T_X$	–	$4T_h$	–
	SN_j	–	–	$3T_h$	–
BTh-UAP 协议	U_i	$5T_h+3T_X+T_{\text{Gen}}$	$5T_h+4T_X+T_{\text{Rep}}+T_E$	$3T_h+2T_X$	所有计算
	GWN	T_h	–	$T_D+2T_h+T_X+T_E$	–
	SN_j	–	–	$T_D+3T_h+2T_X$	–

7 结束语

鉴于生物特征标识的唯一性,有助于提高用户认证协议的安全性. 本文提出了一种基于生物特征标识的三因素 WSN 用户认证协议(BTh-UAP),针对 Althobaiti 协议不能防御节点妥协攻击、网关节点模拟攻击、中间人攻击和内部特权攻击的安全缺陷,以智能卡和密码作为协议基本安全因素,引入生物特征标识;利用 Gen(·)和 Rep(·)函数处理生物特征标识,而不是简单地利用哈希函数;为每个节点配置与网关节点唯一共享密钥,使 GWN 不与所有部署节点共享秘密参数,而由 U_i 选择与 GWN 的共享密钥,提高了公共信道通信的安全性;设计了密码和生物特征标识更新机制,在 GWN 不参与的情况下,U_i 可自由更换密码和生物特征标识. 安全性分析表明,BTh-UAP 可以防御多种安全攻击,实现用户匿名性,保证会话密钥安全与三因素安全,利用 AVIPSA 对协议进行形式化分析与仿真,结果证明 BTh-UAP 克服了 Althobaiti 协议安全缺陷,传感器节点对计算能力的需求小于公钥加密,且具有较低的计算量. 权衡安全性与计算成本,该协议适用于资源受限且安全需求高的 WSN 应用.

本文研究并提出的 BTh-UAP 前提是,WSN 是安全的,传感器节点 SN_j 是合法节点. 若在 BTh-UAP 协议发

起之前,传感器节点 SN_j 被攻击者捕获并妥协,由于 GWN 并不验证节点 SN_j 的合法性,攻击者可以控制节点 SN_j 进行正常通讯,则 U_i 会话密钥将被攻击者获取,因此,本文将以此为主要方向开展后续工作的研究,同时,笔者也注意到当前国内外关于密码(口令)技术的研究,主要围绕着用户脆弱口令行为、口令分布强度评价、口令猜测算法、口令强度评价四个领域的展. 本文后续的另一个主要工作是结合 WSN 节点部署的分布式特性,关注节点分布式协同认证方面的口令猜测算法研究进展.

参考文献

[1] 刘伟,董恩清,宋洋. 无线传感器网络节点三维定位的翻转模糊检测[J]. 电子学报,2016,44(2):374 – 384.
LIU W,DONG E Q,SONG Y. Flip ambiguity detection for three-dimensional node localization in wireless sensor networks[J]. Acta Electronica Sinica,2016,44(2):374 – 384. (in Chinese)

[2] BUTUN I,MORGERA S D,SANKAR R. A survey of intrusion detection systems in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials,2014,16(1):266 – 282.

[3] 李继国,张亦辰,卫晓霞. 可证安全的基于证书广播加密方案[J]. 电子学报,2016,44(5):1101 – 1110.
LI J G,ZHANG Y C,WEI X X. A provably secure certificate-based broadcast encryption scheme[J]. Acta Electronica Sinica,2016,44(5):1101 – 1110. (in Chinese)

[4] 杨鹏,唐洋,舒娜,王汝言. 供给需求关系感知的间断连接无线网络安全路由机制[J]. 通信学报,2015,36(Z1):42 – 52.
YANG P,TANG Y,SHU N,WANG R Y. Secure supply and demand relationship perception routing in intermittently connected wireless networks[J]. Journal on Communications,2015,36(Z1):42 – 52. (in Chinese)

[5] 肖云鹏,姚豪豪,刘宴兵. 一种基于云模型的 WSNs 节点信誉安全方案[J]. 电子学报,2016,44(1):168 – 175.
XIAO Y P,YAO H H,LIU Y B. A WSNs node reputation security scheme based on cloud model[J]. Acta Electronica Sinica,2016,44(1):168 – 175. (in Chinese)

[6] FANG W D,SHAN L H,JIA G Q,JI X H,CHEN S J. A low complexity secure network coding in wireless sensor network[J]. Journal of Internet Technology,2016,17(5):905 – 913.

[7] 李晓伟,张玉清,张格非,刘雪峰,范丹. 基于智能卡的强安全认证与密钥协商协议[J]. 电子学报,2014,42(8):1587 – 1593.
LI X W,ZHANG Y Q,ZHANG G F,LIU X F,FAN D. Strongly secure authenticated key agreement protocol using smart card[J]. Acta Electronica Sinica,2014,42(8):1587 – 1593. (in Chinese)

[8] CHEN X Q,CAO T J,ZHAI J X. Untraceability analysis of two RFID authentication protocols[J]. Chinese Journal of Electronics,2016,25(9):912 – 920.

[9] 刘云,杨亮,范科峰,王勇,唐仕军. 一种改进的动态用户认证协议[J]. 电子学报,2013,41(1):42 – 46.
LIU Y,YANG L,FAN K F,WANG Y,TANG S J. Improved dynamic user authentication protocol[J]. Acta Electronica Sinica,2013,41(1):42 – 46. (in Chinese)

[10] QAZI F A,QAZI F A. A survey of biometric authentication systems[A]. Proceedings of the International Conference on Security and Management,SAM'04[C]. Las Vegas,Nevada,USA:SAM,2004. 61 – 67.

[11] KUMARI S,KHAN M K,ATIQUZZAMAN M. User authentication schemes for wireless sensor networks:A review[J]. Ad Hoc Networks,2015,27:159 – 194.

[12] KAUSHAL K,KAUR T. A survey on attacks of WSN and their security mechanisms[J]. International Journal of Computer Applications,2015,118(18):1 – 4.

[13] LEE J K,RYU S R,YOO K Y. Fingerprint-based remote user authentication scheme using smart cards[J]. Electronics Letters,2002,38(12):554 – 555.

[14] LI C T,HWANG M S. An efficient biometrics-based remote user authentication scheme using smart cards[J]. Journal of Network and computer applications,2010,33(1):1 – 5.

[15] YUAN J,JIANG C,JIANG Z. A biometric-based user authentication for wireless sensor networks[J]. Wuhan University Journal of Natural Sciences,2010,15(3):272 – 276.

[16] LEE C C,CHANG R X,CHEN L A. Improvement of lihwang's biometrics-based remote user authentication scheme using smart cards[J]. WSEAS Transactions on Communications,2011,10(7):193 – 200.

[17] YOON E J,YOO K Y. A new biometric-based user authentication scheme without using password for wireless sensor networks[A]. The 20th IEEE International Workshops on Enabling Technologies:Infrastructure for Collaborative Enterprises (WETICE)[C]. USA:IEEE,2011. 279 – 284.

[18] DAS M L. Two-factor user authentication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications,2009,8(3):1086 – 1090.

[19] SEKHAR V C,SARVABHATLA M. A robust biometric-based three-factor remote user authentication scheme[A]. The Smithsonian/NASA Astrophysics Data System[C]. USA:NASA,2014. arXiv:1401. 1318.

[20] AN Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards[J]. Journal of Biomedicine & Biotechnology,

2012,DOI:10.1155/2012/519723.
[21] CHATURVEDI A,MISHRA D,MUKHOPADHYAY S. Improved Biometric-Based Three-Factor Remote User Authentication Scheme with Key Agreement Using Smart Card[M]. Springer Berlin Heidelberg,2013. 63 – 77.
[22] AWASTHI A K,SRIVASTAVA K. A biometric authentication scheme for telecare medicine information systems with nonce[J]. Journal of Medical Systems,2013,37(5):1 – 4.
[23] LIU X,SHEN Y,LI S,CHEN F. A fingerprint-based user authentication protocol with one-time password for wireless sensor networks[A]. Proceedings of International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS)[C]. Harbin,China:IEEE Press,2013. 9 – 12.
[24] KIANI F,DALKILIC G. Password renewal enhancement for dynamic authentication in wireless sensor networks[A]. Proceedings of the 2nd International Conference on Computational Intelligence,Communication Systems and Networks[C]. Liverpool,United Kingdom:IEEE Press,2010. 143 – 146.
[25] LIU X Y,HUANG T L,WANG X,TANG X J. A user authentication scheme based on dynamic password for wireless sensor networks[A]. Proceedings of International Conference on Intelligent Computing and Integrated Systems (ICISS)[C]. Guilin,China:IEEE Press,2010. 145 – 148.
[26] 喻丽春. 基于 AES 和 RSA 算法的一次性口令认证[J]. 西安邮电大学学报,2017,22(1):38 – 43.
YU L. One-time password authentication based on AES and RSA algorithm[J]. Journal of Xi'an University of Posts and Telecommunications,2017,22(1):38 – 43. (in Chinese)
[27] 韩伟力,袁琅,李思斯,王晓阳. 一种基于样本的模拟口令集生成算法[J]. 计算机学报,2017,40(5):1151 – 1155.
HAN W,YUAN L,LI S,WANG X. An efficient algorithm to generate password sets based on samples[J]. Chinese Journal of Computers,2017,40(5):1151 – 1155. (in Chinese)
[28] 王平,汪定,黄欣沂. 口令安全研究进展[J]. 计算机研究与发展,2016,53(10):2173 – 2188.
WANG P,WANG D,HUANG X. Advances in password security[J]. Journal of Computer Research and Development,2016,53(10):2173 – 2188. (in Chinese)
[29] RAMANUJAM R,SUNDARARAJAN V,SURESH S P. Extending Dolev-Yao with Assertions[M]. Springer International Publishing,2014. 50 – 68.
[30] KIM J,LEE D,JEON W,et al. Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks[J]. Sensors,2014,14(4):6443 – 6462.
[31] HURTADO ALEGRíA J A,BASTARRICA M C,BERGEL A. Avispa: a tool for analyzing software process models[J]. Journal of Software: Evolution and Process,2014,26(4):434 – 450.

作者简介

房卫东　男,1971 年 2 月出生,山东济南人,博士,中国科学院上海微系统与信息技术研究所高级工程师,主要研究方向为无线传感器网络可信传输技术、信任管理、隐私保护.
E-mail:weidong. fang@ mail. sim. ac. cn

张武雄(通信作者)　男,1985 年 5 月出生,湖北孝感人,博士,中国科学院上海微系统与信息技术研究所副研究员,主要研究方向为车联网体系架构及组网技术、异构多网协作.
E-mail:wuxiong. zhang@ mail. sim. ac. cn

杨　旸　男,1974 年 2 月出生,江苏南京人,博士,中国科学院上海微系统与信息技术研究所研究员、博导,主要研究方向为无线传感器网络(物联网)、新一代移动通信系统(5G)、雾计算与网络技术,开放无线测试验证平台.
E-mail:yang. yang@ mail. sim. ac. cn

张传雷　男,1973 年月出生,山东沂源人,博士,天津科技大学计算机科学与信息工程学院副教授,主要研究方向为计算机应用技术、无线传感器网络可信传输技术.
E-mail:97313114@ tust. edu. cn

陈　伟　男,1978 年 9 月出生,江苏徐州人,博士,中国矿业大学计算机科学与技术学院教授,主要研究方向为智能信息处理、无线通信、大数据与云计算.
E-mail:chenw@ cumt. edu. cn