

# 一种可证安全的面向无线传感器网络的双因素用户认证密钥协商方案\*

陈蕾, 魏福山, 马传贵

(解放军信息工程大学 数学工程与先进计算国家重点实验室, 郑州 450001)

**摘要:** 随着无线传感器网络的快速发展, 对外部用户的身份进行确认已成为获取传感器网络中实时数据所要解决的关键问题。在对无线传感器网络中双因素用户认证密钥协商方案系统的研究基础上, 指出 Kalra 的用户认证方案存在安全缺陷, 随后针对于现实应用中敌手的能力提出一种新的可证安全方案。新方案在满足用户匿名性的同时, 能达到真正的双向认证, 并在针对 WSN 的双因素认证方案安全模型中给出安全性证明。与已有的同类方案对比, 该方案具有更高的安全性和效率, 更适合资源受限环境及现实应用。

**关键词:** 无线传感器网络; 用户认证; 口令; 智能卡; 会话密钥建立

**中图分类号:** TP393.04    **文献标志码:** A    **文章编号:** 1001-3695(2016)05-0001-08

doi:10.3969/j.issn.1001-3695.2016.05.052

## Provably-secure two-factor user authentication key exchange scheme for wireless sensor networks

Chen Lei, Wei Fushan, Ma Chuangui

(State Key Laboratory of Mathematical Engineering & Advanced Computing, PLA Information Engineering University, Zhengzhou 450001, China)

**Abstract:** With the development of wireless sensor network (WSN), user authentication in WSN is a critical security issue due to their unattended and hostile deployment in the field. In order to protect the security of real-time data query from an external user, many papers proposed two factor (password and smart-card) user authentication schemes. In this paper, we reviewed the scheme proposed by Kalra *et al.* It firstly found that the scheme was vulnerable. It proposes a robust and efficient password based authentication scheme which was secure against all well-known security attacks, and proved its security properties in Nam's extended model. Security and performance analysis demonstrate that compared to the existing schemes, this proposal is more secure and efficient.

**Key words:** wireless sensor network (WSN); user authentication; password; smart-card; session key establishment

## 0 引言

近年来, 无线传感器网络(WSN)上的技术及其应用得到了快速的发展, 呈现空前的繁荣景象。传感器网络通常由大量低成本、低功耗且资源有限的传感器节点组成, 其目的是协作地感知、采集、处理和传输网络覆盖地理区域内感知对象的检测信息, 并报告给用户。由于无线传感器具有经济可行和实时监测的特点, 已得到了广泛的应用, 如军事侦察、环境监测、医疗健康和空间探索等。实际应用时, 要求其能够对访问无线传感器网络的用户身份进行确认, 确保其合法性。访问控制是对信息资源进行保护的重要措施, 它决定了谁能够访问系统, 能访问系统的何种资源以及如何使用这些资源。用户认证是最基本的访问控制方法。

2009年Das<sup>[1]</sup>提出了首个基于智能卡和口令的双因素用户认证方案, 然而此协议被指出存在多种安全缺陷, 如特权内

部人攻击<sup>[2~4]</sup>、离线字典攻击<sup>[5,6]</sup>、节点捕获攻击<sup>[4~8]</sup>等。随后越来越多的基于Das方案改进的双因素用户认证方案<sup>[2~20]</sup>相继被提出, 如文献[3]、[5]等。2010年, Vaidya<sup>[8]</sup>等人指出K-A方案存在智能卡泄露攻击和网关旁路攻击, 并对其作出改进。2011年, Fan等人<sup>[14]</sup>提出了可以抵抗拒绝服务攻击的用户认证方案。9年, Yuan<sup>[9]</sup>添加生物因素, 提出了基于指纹的用户认证方案。为了提高安全性, Yeh等人<sup>[16]</sup>在2011年引用了椭圆曲线密码体制。在这些面向无线传感器的双因素用户认证方案中, 早期的方案主要侧重于双向认证<sup>[2,3]</sup>, 随后越来越多的方案设计满足多种安全性能, 如密钥交换<sup>[12,15~18]</sup>、用户匿名性<sup>[18]</sup>等, 一些方案利用椭圆曲线密码体制<sup>[16,17]</sup>提供更高的安全性, 而大多数方案仅使用对称密码体制及哈希函数以确保拥有更高的效率。然而设计一个具有可证明安全的面向无线传感器网络的双因素用户认证方案仍然是一个公开性的难题。2014年Nam等人<sup>[20]</sup>提出了专门针对于此类方案的安全

收稿日期: 2015-03-07; 修回日期: 2015-03-03    基金项目: 国家自然科学基金资助项目(61379150, 61309016); 河南省自然科学基金资助项目(122102210426); 信息保障技术重点实验室开放课题(KJ-13-02); 国家“十二五”密码发展基金资助项目(MMJ201201005)

**作者简介:** 陈蕾(1990-), 女, 湖北襄阳人, 硕士研究生, 主要研究方向为安全协议的设计与分析(chenleixy0730@163.com); 魏福山(1983-), 男, 甘肃武威人, 讲师, 博士, 主要研究方向为安全协议的设计与分析; 马传贵(1962-), 男, 山东菏泽人, 教授, 博导, 博士, 主要研究方向为密码协议、无线通信。

模型,但该模型仍然需要继续完善。

值得一提的是,2013 年,Xue 等人<sup>[18]</sup>提出了一个基于临时证书的双向认证密钥协商方案。2014 年 Kalra 等人<sup>[19]</sup>指出 Xue 的方案存在安全缺陷,如不能抵抗仿冒攻击、智能卡泄露攻击,且具有不合理的假设、错误的登录阶段等,并基于 Xue 的方案进行了改进。然而本文对 Kalra 方案进行安全性分析后发现,该方案仍然存在很多漏洞,如未达到双向认证、未满足前向安全性、存在用户仿冒攻击等安全缺陷。

本文将基于 Kalra 的方案,针对资源受限的无线传感器网络环境以及现实应用中敌手的能力,提出一个可证安全的双因素用户认证密钥协商方案。该方案满足用户匿名性,达到了用户、网关节点、传感器节点三者之间的双向认证,可以抵抗多种已知攻击,并且建立了满足前向安全性的会话密钥。本文将基于 Nam 的安全模型,对其进行安全性证明。与其他现存方案相比,提出的新方案拥有更高的安全性,且计算量小、通信成本低、更高效,适合资源受限环境及现实应用。

## 1 Kalra 方案回顾

本章将回顾 Kalra 等人<sup>[19]</sup>提出的无线传感器网络用户认证协议,此方案中包含注册、登录、认证及密钥建立和口令更新四个阶段。

### 1.1 注册阶段

当用户想要访问无线传感器网络,它必须在网关节点处注册。其具体步骤如下:

a) 用户  $U_i$  选择随机数  $n$ ,计算安全参数  $E_i = H(ID_i \parallel n)$  和  $F_i = H(P_i \oplus n)$ 。其中: $ID_i$  是用户  $U_i$  的身份标志, $P_i$  是用户  $U_i$  的口令,并将  $E_i$  和  $F_i$  通过安全信道传给 GWN。

b) GWN 计算安全参数  $G_i = E_i \oplus y_i$ ,  $H_i = F_i \oplus H(y_i) \oplus x$  及  $J_i = E_i \oplus H(y_i) \oplus x$ 。其中: $x$  是 GWN 的秘密值, $y_i$  是 GWN 为用户  $U_i$  所选的随机值。GWN 将  $y_i \oplus x$  对应  $J_i$  存储在客户数据库中,并将  $(G_i, H_i, H(\cdot))$  写入智能卡中,通过安全信道发给用户。

c) 用户收到智能卡后计算  $A_i = n \oplus H(ID_i \parallel P_i)$  和  $B_i = H(ID_i \parallel P_i) \oplus P_i$ ,并将  $A_i$  和  $B_i$  写入智能卡中。

每个在传感器网络中的传感器节点也必须在网关节点处注册,即传感器节点  $S_s$  与 GWN 共同商定一个特有密钥  $SK_s$ 。GWN 将  $SK_s \oplus H(x \parallel SID_s)$  对应  $SID_s$  存储在服务器数据库中,其中  $SID_s$  表示传感器节点  $S_s$  的身份标志。

### 1.2 登录阶段

如果用户想要获取传感器网络收集的信息,需要把智能卡插入终端,并输入  $ID_i^*$  和口令  $P_i^*$ 。智能卡验证用户身份。具体步骤如下:

a) 智能卡计算  $B_i^* = H(ID_i^* \parallel P_i^*) \oplus P_i^*$ ,并验证  $B_i^*$  是否与存储在智能卡上的  $B_i$  相等。如果相等,用户合法性得到验证,继续以下操作,否则终止协议。

b) 智能卡生成一次性随机数  $N_1$ ,并计算  $n = A_i \oplus H(ID_i \parallel P_i)$ ,  $E_i = H(ID_i \parallel n)$ ,  $F_i = H(P_i \oplus n)$ ,  $y_i = E_i \oplus G_i$ ,  $H(x) = F_i \oplus H(y_i) \oplus H_i$ ,  $C_i = H^2(x) \oplus N_1$ ,  $CID_i = E_i \oplus H(y_i) \oplus H(x) \oplus N_1$  和  $K_i = H(H(x) \parallel y_i \parallel N_1)$ 。 $U_i$  将登录请求  $(C_i \parallel CID_i \parallel K_i)$  发送给 GWN。

c) GWN 将登录请求转发给距离最近的可用传感器节点  $S_s$ 。

### 1.3 认证及密钥建立阶段

当  $S_s$  收到经由 GWN 转发的用户  $U_i$  登录请求后,将进行双向认证和密钥建立。具体操作如下:

a) 传感器节点  $S_s$  生成一次性随机数  $N_2$ ,计算  $D_i = N_2 \oplus SK_s$ ,并将登录请求  $(SID_s, C_i, CID_i, K_i, D_i)$  发送给 GWN。

b) GWN 从数据库  $SID_s$  对应的  $SK_s \oplus H(x \parallel SID_s)$  中提取出密钥  $SK_s$ ,计算  $N_1 = C_i \oplus H^2(x)$ ,  $N_2 = D_i \oplus SID_s$ ,  $J_i^* = CID_i \oplus N_1 \oplus H(x) \oplus x$ ,并从数据库中找到与  $J_i^*$  相匹配的  $J_i$  值,若能找到匹配的值,继续以下操作,否则拒绝其登录请求。

c) GWN 利用数据库从  $J_i^*$  相对应的  $y_i \oplus x$  中提取出  $y_i$ ,计算  $K_i^* = H(H(x) \parallel y_i \parallel SID_s \parallel N_1)$ 。对比  $K_i^*$  与接收到的  $K_i$  值是否相等以验证用户和传感器节点  $S_s$  的合法性。若相等,继续以下操作,否则拒绝登录请求并中止会话。

d) GWN 生成一次性随机数  $N_3$ ,计算  $M_i = N_1 \oplus N_3 \oplus H(SK_s \parallel N_2)$ ,  $R_i = H(CID_i \parallel y_i \parallel N_1) \oplus H(N_1 \oplus N_2 \oplus N_3)$ ,  $V_i = H(H(N_1 \oplus N_2 \oplus N_3) \parallel H(CID_i \parallel y_i \parallel N_1))$ ,  $W_i = N_2 \oplus N_3 \oplus H(y_i \parallel CID_i \parallel H(x) \parallel N_1)$ ,并将  $(M_i, R_i, V_i, W_i)$  发送给传感器节点  $S_s$ 。

e) 传感器节点收到消息后计算  $N_1 \oplus N_3 = M_i \oplus H(SK_s \parallel N_2)$ ,  $H(CID_i \parallel y_i \parallel N_1) = R_i \oplus H(N_1 \oplus N_2 \oplus N_3)$ ,并利用这些值计算  $V_i^* = H(H(N_1 \oplus N_2 \oplus N_3) \parallel H(CID_i \parallel y_i \parallel N_1))$ ,对比其与收到的  $V_i$  是否相等以验证 GWN 的合法性。若相等,则将  $(V_i, W_i)$  发送给用户  $U_i$ ,否则中止会话。

f) 智能卡收到  $(V_i, W_i)$  后,计算  $N_2 \oplus N_3 = W_i \oplus H(y_i \parallel CID_i \parallel H(x) \parallel N_1)$ ,  $V_i^* = H(H(N_1 \oplus N_2 \oplus N_3) \parallel H(CID_i \parallel y_i \parallel N_1))$ ,并其与收到的  $V_i$  是否相等以验证 GWN 和  $S_s$  的合法性。

完成以上认证后,用户  $U_i$ 、传感器节点  $S_s$  以及网关节点 GWN 之间建立一个共同的会话密钥  $SK = H(H(ID_i \parallel y_i \parallel N_1) \parallel (N_1 \oplus N_2 \oplus N_3))$ 。

### 1.4 口令更新阶段

如果用户  $U_i$  想要更新口令,插入智能卡,输入  $ID_i^*$  和口令  $P_i^*$ ,智能卡计算  $B_i^* = H(ID_i^* \parallel P_i^*) \oplus P_i^*$ ,并验证  $B_i^*$  是否与存储在智能卡上的  $B_i$  相等以验证用户身份的合法性。合法性得到验证后用户提交新的口令  $P_i^{new}$ ,智能卡计算  $n = H(y_i) \parallel H(x)$ ,并更新  $A_i^{new} = n \oplus H(ID_i \parallel P_i^{new})$ ,  $B_i^{new} = H(ID_i \parallel P_i^{new}) \oplus P_i^{new}$  和  $H_i^{new} = H(P_i^{new} \oplus n) \oplus H(y_i) \oplus H(x)$ ,此时完成口令更新阶段。

## 2 Kalra 方案的安全性分析

Kalra 指出他们的方案能抵抗各种攻击,但是通过分析,笔者发现 Kalra 方案仍然存在安全漏洞,如存在节点仿冒攻击、用户仿冒攻击、未满足前向安全性等。在给出安全性分析前,先定义敌手的能力。假设敌手能够控制整个通信网络,且拥有以下能力:敌手可以读取、修改、插入、删除、重放和延迟公共网络中传递的消息信息;敌手可以获取用户的口令,也可以窃取用户智能卡并提取利用存储的秘密值,但两者不能同时兼具;敌手可以捕获传感器节点  $S_s$  并提取利用其中秘密值。

### 2.1 未达到双向认证/节点仿冒攻击

在 Kalra 方案的认证及密钥建立阶段,GWN 在收到传感器节点  $S_s$  发送过来的  $D_i = N_2 \oplus SK_s$  后,并没有验证  $S_s$  的合法

性,而是直接计算出  $N_2$  并继续下步操作。Kalra 称在 1.3 节步骤 f) 中用户检验  $V_i^* = H(H(N_1 \oplus N_2 \oplus N_3) \parallel H(CID_i \parallel y_i \parallel N_1))$  与收到的  $V_i$  是否相等来同时验证 GWN 和  $S_s$  的合法性。然而用户利用  $V_i$  来验证  $S_s$  的这种方式是无效的。假设  $S_s$  是恶意的或被敌手捕获,  $S_s$  只需要在 1.3 节步骤 a) 中随机生成一个  $D_i$ , 并在步骤 e) 收到 GWN 发来的消息后直接转发 ( $V_i$ ,  $W_i$ ) 给用户, 便可通过用户的认证。因此,  $S_s$  的合法性并没有得到验证, 敌手能轻易地仿冒传感器节点, 即 Kalra 方案不满足用户、网关节点与传感器节点之间的双向认证。

## 2.2 未满足前向安全性/智能卡丢失引起的密钥泄露

传感器网络中满足完美的前向安全性是指三个参与者(用户  $U_i$ 、网关节点 GWN、传感器节点  $S_s$ ) 的私钥泄露后不会对之前建立的会话密钥安全性产生影响, 主要分为完美前向安全(p-FS) 和主密钥完美前向安全。p-FS 是指用户和传感器节点的私钥同时泄露不会对之前建立的会话密钥安全性产生影响, 主密钥完美前向安全是指服务器(即网关节点 GWN) 的主密钥泄露不会对之前建立的会话密钥安全性产生影响。本文通过分析得出, Kalra 的方案不满足 p-FS。具体的攻击如下所示:

假设  $U_j$  是另一个已注册的合法用户, 则  $U_j$  可以利用自己的智能卡恢复出  $H(x) = F_j \oplus H(y_j) \oplus H_j$ 。若  $U_j$  设法读取了  $U_i$  在公共信道传递的消息  $(C_i \parallel CID_i \parallel K_i)$ , 并窃取了  $U_i$  的智能卡利用其中秘密值  $(A_i, B_i, G_i, H_i, H(\cdot))$ , 那么  $U_j$  可以恢复出  $U_i$  的所有秘密值(除口令外)。

$$\begin{aligned} F_i &= H(A_i \oplus B_i) = H(P_i \oplus n) \\ H(y_i) &= H(x) \oplus F_i \oplus H_i \\ N_1 &= H^2(x) \oplus C_i \\ E_i &= CID_i \oplus H(y_i) \oplus H(x) \oplus N_1 \\ y_i &= E_i \oplus G_i \end{aligned}$$

假设  $(C'_i \parallel CID'_i \parallel K'_i)$  和  $(V'_i, W'_i)$  是此前用户  $U_i$  参与的某次会话在公共信道上传输的消息, 那么敌手即可计算出  $N'_1 = H^2(x) \oplus C'_i$ ,  $N'_2 \oplus N'_3 = W'_i \oplus H(y_i \parallel CID'_i \parallel H(x) \parallel N'_1)$ , 从而得到会话密钥  $SK' = H(H(CID'_i \parallel y_i \parallel N'_1) \parallel (N'_1 \oplus N'_2 \oplus N'_3))$ 。

因此在 Kalra 方案中, 用户智能卡的泄露会导致用户私钥的泄露, 从而对之前建立的会话密钥安全性产生影响, 不具备会话密钥的完美前向安全性。

## 2.3 用户仿冒攻击

在 Kalra 方案中, 假设  $U_j$  是窃取到  $U_i$  智能卡的恶意合法用户, 如 2.2 小节中所示, 则  $U_j$  可以利用计算出来的  $U_i$  的秘密值, 随机选取某随机数  $N_1$ , 便可计算出合法的登录信息  $(C_i \parallel CID_i \parallel K_i)$  并发送至 GWN。在认证及密钥建立阶段, GWN 验证用户  $U_j$  的合法身份时, 计算  $J_i^* = CID_i \oplus N_1 \oplus H(X) \oplus x$ , 并从数据库中找到与  $J_i^*$  相匹配的  $J_i$  值, 从而通过验证。

在 Kalra 的注册阶段, GWN 为达到匿名性, 将  $y_i \oplus x$  对应  $J_i$  存储在客户数据库中, 并未涉及到用户的身份信息  $ID_i$ 。因此, GWN 验证用户  $U_j$  的合法身份时, 计算  $J_i^* = CID_i \oplus N_1 \oplus H(X) \oplus x$  后从数据库中找到与  $J_i^*$  相匹配的  $J_i$  值, 而并非匹配的是原本的  $J_j$  值。虽然网关节点 GWN 对已注册的合法用户身份不作区分, 但从某种意义上讲, 用户  $U_j$  仍然成功仿冒了用户  $U_i$ , 因此 Kalra 方案存在智能卡丢失引起的用户仿冒攻击。

## 2.4 错误的验证方式

在 Kalra 方案的设计中, 用户在登录阶段计算  $K_i = H(H(x) \parallel y_i \parallel N_1)$  并发送给 GWN, 在认证及密钥建立阶段, GWN 通过计算  $K_i^* = H(H(x) \parallel y_i \parallel SID_s \parallel N_1)$ , 对比  $K_i^*$  与接收到的  $K_i$  值是否相等以验证用户和传感器节点  $S_s$  的合法性。在这里无论用户和传感器节点  $S_s$  合法与否, 都无法得到  $K_i^* = K_i$ 。

## 2.5 错误的会话密钥计算

在 Kalra 方案的设计中, 最终的会话密钥是  $SK = H(H(ID_i \parallel y_i \parallel N_1) \parallel (N_1 \oplus N_2 \oplus N_3))$ , 而此时 GWN 和传感器节点  $S_s$  是无法得知用户的身份  $ID_i$ , 也无法计算出  $H(ID_i \parallel y_i \parallel N_1)$  等值, 因此给出的会话密钥计算式是错误的, 也是无效的。

## 3 安全模型

Nam 在文献[20]中针对无线传感器网络上双因素用户认证及密钥协商方案提出了安全模型, 该模式是在 BPR 模型的基础上进行扩展, 本文也将利用此模型对新提出的协议进行安全性证明。在提出新的协议之前, 本文将 Nam 的模型回顾如下:

**参与者:** GW 表示网关节点; 令  $S$  和  $U$  分别表示所有在 GW 处注册过的传感器节点和用户的集合。令  $\varepsilon = \{GW\} \cup U \cup S$ , 每个实体的身份可以用  $E \in \varepsilon$  或者  $ID_E$  来标志。一个用户  $U \in U$  可以与某个传感器节点  $S \in S$  同时运行多个认证及密钥建立会话, 这些会话经由一个共同的网关节点 GW。

**会话实例:** 任何一个时间点, 在某个用户  $U \in U$ 、传感器节点  $S \in S$  及网关 GW 之间可能存在多个会话实例。用  $\Pi_E^i$  来表示某个实体  $E \in \varepsilon$  的第  $i$  个会话实例, 用  $sk_E^i$  表示实例  $\Pi_E^i$  中计算出来的会话密钥。如果用户  $U \in U$  或传感器节点  $S \in S$  的会话实例计算出了会话密钥, 则称为实例是被接受的。

在协议运行前, 作以下规定:

a) GW 已拥有自己的主密钥, 为每个用户  $U \in U$  颁发一个智能卡, 并与每个传感器节点  $S \in S$  建立一个共享密钥。

b) 每个用户  $U \in U$  在相应的口令空间中选择个人私有的口令  $PW$ 。

**伙伴:** 若两个参与者运行了协议, 并建立了一个共享密钥, 则称这两个参与者的实例为伙伴。可以用会话标志的概念来详细定义伙伴, 即会话标志(sid)指一个协议会话的身份标志, 包含了这个会话中所有交换的消息、所用的函数等信息, 我们用  $sid_E^i$  表示实例  $\Pi_E^i$  会话 sid 的会话标识。如果实例  $\Pi_U^i$  和  $\Pi_S^i$  是伙伴, 当且仅当满足两个条件:a) 两个实例都是被接受的;b)  $sid_U^i = sid_S^i$ 。

**敌手能力:** 定义 A 是一个概率多项式时间的敌手, 可以控制实体之间所有的通信。即敌手 A 拥有以下能力:a) 窃听、修改、插入、延迟及删除协议通信中的消息;b) 获取实体的长期密钥及某次会话的会话密钥;c) 获取用户智能卡中存储的秘密信息值。敌手的这些能力可以通过一系列的预言机来定义, 描述如下:

a)  $\text{Execute}(\Pi_U^i, \Pi_S^i, \Pi_{CW}^i)$ , 这个查询主要反映敌手被动窃听的能力。它可以使实例  $\Pi_U^i$ 、 $\Pi_S^i$  与  $\Pi_{CW}^i$  之间完成一次协议的运行, 并且将这次协议运行的副本返回给敌手 A。

b)  $\text{Send}(\Pi_E^i, m)$ , 这个查询使其在实例  $\Pi_E^i$  中发送消息  $m$ ,

主要反映的是敌手主动攻击的能力。当收到消息  $m$  后, 实例  $\Pi_E^i$  根据协议的程序规则生成相应的输出, 并返回给敌手  $A$ 。如果格式为  $\text{Send}(\Pi_U^i, \text{start})$ , 则表示令  $\Pi_U^i$  创建了一个初始协议会话。

c)  $\text{Reveal}(\Pi_E^i)$ , 这个查询反映的是已知密钥攻击。当收到这个查询请求时, 实例  $\Pi_E^i$  如果是被接受的, 则将其会话密钥  $sk_E^i$  返回给敌手  $A$ 。

d)  $\text{CorruptLL}(E)$ , 这个查询反映的是前向安全性, 未知密钥共享攻击以及内部人攻击。收到这个查询请求时, 将实体  $E$  的长期密钥返回给敌手  $A$ 。

e)  $\text{CorruptSC}(U)$ , 这个查询反映的是侧信道攻击。收到这个查询请求时, 将用户  $U$  智能卡中存储的秘密信息值返回给敌手  $A$ 。

f)  $\text{TestAKE}(\Pi_E^i)$ , 这个查询主要用于定义会话密钥不可区分安全性。预言机选取一个随机值  $b$ , 当  $b = 1$  时, 则将真实的会话密钥  $sk_E^i$  返回给敌手  $A$ ; 否则  $b = 0$ , 从会话密钥空间里随机选取一个随机数返回给敌手  $A$ 。

注: 若对传感器节点  $S$  和网关节点  $GW$  作出  $\text{CorruptLL}$  查询, 则称  $S$  和  $GW$  被腐化。若用户  $U$  称做被腐化时, 必须同时对其作  $\text{CorruptLL}$  和  $\text{CorruptSC}$  查询。

认证密钥交换(AKE): 在认证及密钥交换协议中, 本文用实例的新鲜性概念来定义 AKE 安全。一个新鲜的实例是指对于敌手  $A$  来说, 这个实例的会话密钥和一个随机密钥具有不可区分性; 而一个不新鲜的实例是指敌手  $A$  能通过一些手段, 将此实例的会话密钥与一个随机密钥区分出来。新鲜性的定义如下:

定义 1 新鲜性。假设实例  $\Pi_E^i$  的参与者为用户  $U \in U$ 、网关节点  $GW$  与传感器节点  $S \in S$ , 若实例  $\Pi_E^i$  称做是新鲜的, 当且仅当满足以下条件:

a) 敌手  $A$  不能做  $\text{Reveal}(\Pi_E^i)$  或  $\text{Reveal}(\Pi_E^i)$  查询, 其中实例  $\Pi_E^i$  是  $\Pi_E^i$  的伙伴。

b) 在实例  $\Pi_E^i$  被接受前, 敌手  $A$  不能做  $\text{CorruptLL}(S)$  或  $\text{CorruptLL}(GW)$  查询。

c) 在实例  $\Pi_E^i$  被接受前, 敌手  $A$  不能对用户  $U$  同时做  $\text{CorruptLL}(U)$  和  $\text{CorruptSC}(U)$  查询。

协议 P 的 AKE 安全性可以通过两个阶段的实验来定义。

实验  $\text{ExpAKE}_0$ :

阶段 1 敌手  $A$  可以对任何预言机进行查询, 除了以下两个限制:

a) 如果  $\Pi_E^i$  是不新鲜的, 则敌手  $A$  不允许进行  $\text{TestAKE}(\Pi_E^i)$  查询;

b) 在进行  $\text{TestAKE}(\Pi_E^i)$  查询后, 给出猜测结果(阶段 2)之前, 要始终保证  $\Pi_E^i$  的新鲜性。

阶段 2 当阶段 1 结束后, 敌手  $A$  输出值  $b'$ , 作为对查询  $\text{TestAKE}(\Pi_E^i)$  中随机值  $b$  的猜测。如果  $b' = b$ , 则表示敌手  $A$  赢得了这次实验。

令  $\text{SuccAKE}_0$  表示敌手  $A$  赢得了实验  $\text{ExpAKE}_0$  这个事件, 令  $\text{Adv}_P^{\text{AKE}}(A)$  定义为敌手  $A$  破坏了协议 P 的 AKE 安全性的优势, 则  $\text{Adv}_P^{\text{AKE}}(A) = 2 \cdot \Pr_{P,A}[\text{SuccAKE}_0] - 1$ 。

定义 2 AKE 安全性。认证及密钥交换协议 P 是 AKE 安全的当且仅当  $\text{Adv}_P^{\text{AKE}}(A)$  对于概率多项式时间的敌手  $A$  来说

是可忽略的。

## 4 一种改进的方案/新方案描述

基于 Kalra 方案的安全缺陷, 本文将提出一个新的无线传感器网络下的双因素用户认证密钥交换协议。该方案克服了 Kalra 中存在的安全隐患, 满足用户、网关节点及传感器节点之间的双向认证, 并建立会话密钥。新方案由注册、登录、认证及密钥建立和口令更新四部分组成。

### 4.1 注册阶段

当用户想要访问无线传感器网络时, 它必须先在网关节点注册。用户把身份和口令提交给网关节点  $GWN$ ,  $GWN$  给用户颁发一个合法的智能卡, 如附录中图 1 所示。具体步骤如下:

a) 用户  $U_i$  选择口令  $PW_i$  和随机数  $b$ , 然后通过安全信道将身份  $ID_i = h(ID_i \parallel b)$  和  $\overline{PW}_i = h(PW_i \parallel b)$  发送给  $GWN$ 。

b)  $GWN$  计算安全参数  $G_i = \overline{ID}_i \oplus \overline{PW}_i \oplus y_i$  及  $H_i = \overline{PW}_i \oplus H(y_i) \oplus H(x)$ 。其中:  $x$  是  $GWN$  的秘密值,  $y_i$  是  $GWN$  为用户  $U_i$  所选的随机值。 $GWN$  将  $y_i \oplus x$  对应  $\overline{ID}_i$  存储在客户数据库中, 并将  $\{G_i, H_i, H(\cdot)\}$  写入智能卡中, 通过安全信道发给用户。然后  $GWN$  从内存中删除  $\overline{ID}_i, \overline{PW}_i, G_i, H_i$ 。

c) 用户收到智能卡后计算  $A_i = b \oplus H(ID_i \parallel PW_i)$  和  $B_i = H(PW_i \parallel ID_i) \oplus H(PW_i \oplus b)$ , 并将  $A_i$  和  $B_i$  写入智能卡中。

### 4.2 登录阶段

如果用户想要获取传感器网络收集的信息, 需要把智能卡插入终端, 并输入  $ID_i$  和口令  $PW_i$ 。智能卡需要验证用户身份。具体步骤如下:

a) 智能卡计算  $b^* = A_i \oplus H(ID_i \parallel PW_i)$ ,  $B_i^* = H(PW_i \parallel ID_i) \oplus H(PW_i \oplus b^*)$ , 并验证  $B_i^*$  是否与存储在智能卡上的  $B_i$  相等。如果相等, 用户合法性得到验证, 继续以下操作, 否则终止协议。

b) 智能卡生成一次性随机数  $N_1$ , 并计算  $y_i = G_i \oplus \overline{ID}_i \oplus \overline{PW}_i, H(x) = H_i \oplus \overline{PW}_i \oplus H(y_i), C_i = H(x) \oplus y_i \oplus N_1$  和  $K_i = H(H(x) \parallel y_i \parallel N_1 \parallel \overline{ID}_i)$ 。 $U_i$  将登录请求  $\{\overline{ID}_i, C_i, K_i\}$  发送给  $GWN$ 。

c)  $GWN$  将登录请求转发给距离最近的可用传感器节点  $S_s$ 。

### 4.3 认证及密钥建立阶段

$S_s$  收到经由  $GWN$  转发的用户  $U_i$  登录请求后, 将进行双向认证和密钥建立。具体操作如下:

a) 传感器节点  $S_s$  生成一次性随机数  $N_2$ , 计算  $D_i = N_2 \oplus h(x \parallel SID_s), E_i = H(\overline{ID}_i \parallel C_i \parallel K_i \parallel D_i \parallel SID_s \parallel h(x \parallel SID_s))$ 。其中  $h(x \parallel SID_s)$  是  $S_s$  与  $GWN$  共享的秘密值, 事先存储在  $S_s$  中。而后  $S_s$  将登录请求  $\{\overline{ID}_i, C_i, K_i, SID_s, D_i, E_i\}$  发送给  $GWN$ 。

b)  $GWN$  利用数据库从  $\overline{ID}_i$  相对应的  $y_i \oplus x$  中提取出  $y_i$ , 计算  $N_1^* = C_i \oplus H(x) \oplus y_i, K_i^* = H(H(x) \parallel y_i \parallel N_1^* \parallel \overline{ID}_i)$ , 对比  $K_i^*$  与接收到的  $K_i$  值是否相等以验证用户的合法性。若相等, 继续以下操作, 否则拒绝登录请求并中止会话。

c)  $GWN$  计算  $E_i^* = H(\overline{ID}_i \parallel C_i \parallel K_i \parallel D_i \parallel SID_s \parallel h(x \parallel SID_s))$ , 对比  $E_i^*$  与接收到的  $E_i$  值是否相等以验证传感器节点  $S_s$  的合法性。若相等, 计算  $N_2 = D_i \oplus h(x \parallel SID_s)$ , 并继续以下操作, 否则中止会话。

d)  $GWN$  生成一次性随机数  $N_3$ , 计算  $W_i = N_2 \oplus N_3 \oplus$

$H(y_i \parallel H(x) \parallel N_1 \parallel \overline{ID}_i)$ ,  $V_i = H(H(N_1 \oplus N_2 \oplus N_3) \parallel H(y_i \parallel N_1 \parallel \overline{ID}_i))$ ,  $M_i = N_1 \oplus N_3 \oplus H(h(x \parallel SID_s) \parallel N_2)$ ,  $R_i = H(\overline{ID}_i \parallel y_i \parallel N_1) \oplus H(N_1 \oplus N_2 \oplus N_3)$ ,  $F_i = H(R_i \parallel H(N_1 \oplus N_2 \oplus N_3) \parallel SID_s \parallel h(x \parallel SID_s))$ , 并将  $\{W_i, V_i, M_i, R_i, F_i\}$  发送给传感器节点  $S_s$ 。

e) 传感器节点收到消息后计算  $N_1 \oplus N_3^* = M_i \oplus H(h(x \parallel SID_s) \parallel N_2)$ ,  $F_i^* = H(R_i \parallel H((N_1 \oplus N_3)^* \oplus N_2) \parallel SID_s \parallel h(x \parallel SID_s))$ , 对比其与收到的  $F_i$  是否相等以验证 GWN 的合法性。若相等, 则继续以下操作, 否则中止会话。

f) 传感器节点计算  $H(\overline{ID}_i \parallel y_i \parallel N_1) = R_i \oplus H(N_1 \oplus N_2 \oplus N_3)$ ,  $S_i = H(W_i \parallel V_i \parallel H(\overline{ID}_i \parallel y_i \parallel N_1) \parallel H(N_1 \oplus N_2 \oplus N_3))$ , 并将  $\{W_i, V_i, S_i\}$  发送给用户  $U_i$ 。

g) 用户  $U_i$  收到  $\{W_i, V_i, S_i\}$  后, 计算  $N_2 \oplus N_3^* = W_i \oplus H(y_i \parallel H(x) \parallel N_1 \parallel \overline{ID}_i)$ ,  $V_i^* = H(H(N_1 \oplus (N_2 \oplus N_3)^*) \parallel H(y_i \parallel N_1 \parallel \overline{ID}_i))$ , 并检验其与收到的  $V_i$  是否相等以验证 GWN 的合法性。若相等, 则计算  $S_i^* = H(W_i \parallel V_i \parallel H(\overline{ID}_i \parallel y_i \parallel N_1) \parallel H(N_1 \oplus N_2 \oplus N_3))$ , 并对比其与收到的  $S_i$  是否相等以验证  $S_s$  的合法性, 且确认  $S_s$  是否算出正确会话密钥值, 否则中止会话。

完成以上认证后, 用户  $U_i$ 、传感器节点  $S_s$  以及网关节点 GWN 之间建立一个共同的会话密钥。先计算中间秘密值  $K = H((N_1 \oplus N_2 \oplus N_3) \parallel H(\overline{ID}_i \parallel y_i \parallel N_1))$ , 最后计算会话密钥  $SK = H(K \parallel C_i \parallel D_i \parallel E_i \parallel F_i \parallel W_i \parallel V_i)$ 。

登录阶段、认证及会话密钥建立阶段如附录中图 2 所示。

#### 4.4 口令更新阶段

如果用户  $U_i$  想要更新口令, 插入智能卡, 输入  $ID_i$  和口令  $PW_i$ , 智能卡计算  $b^* = A_i \oplus H(ID_i \parallel PW_i)$ ,  $B_i^* = H(PW_i \parallel ID_i) \oplus h(PW_i \oplus b^*)$ , 并验证  $B_i^*$  是否与存储在智能卡上的  $B_i$  相等以验证用户身份的合法性。合法性得到验证后用户提交新的口令  $PW_i^{new}$ , 智能卡计算  $\overline{PW}_i = h(PW_i \parallel b^*)$  和  $PW_i^{new} = h(PW_i^{new} \parallel b^*)$ , 并更新  $A_i^{new} = b^* \oplus H(ID_i \parallel PW_i^{new})$ ,  $B_i^{new} = H(PW_i^{new} \parallel ID_i) \oplus H(PW_i^{new} \oplus b^*)$ ,  $G_i^{new} = G_i \oplus \overline{PW}_i \oplus PW_i^{new}$  和  $H_i^{new} = H_i \oplus \overline{PW}_i \oplus PW_i^{new}$ , 此时完成口令更新阶段。

### 5 安全性证明及性能分析

#### 5.1 安全性证明

本节给出新方案 P 在 Nam 模型中的安全性证明。

定理 1 假设方案 P 中的 Hash 函数是安全的, 那么方案 P 是 AKE 安全的, 即概率多项式时间的敌手 A 的破坏方案 P 的 AKE 安全的优势  $\text{Adv}_P^{\text{AKE}}(A)$  是可忽略的。

证明 对于此定理的证明采用归约证明的方法。证明由一系列混合实验组成, 从代表真实协议运行的攻击实验开始, 到敌手优势为 0 的实验结束。在每一个实验中, 逐步修改会话密钥生成的方式。首先用随机数替代被动攻击中的会话密钥; 然后修改主动攻击中的会话密钥, 到最后一个实验, 所有的会话密钥完全随机, 因此敌手无法区分真实的会话密钥和与会话密钥等长的随机数; 最后通过两个相邻的实验之间敌手优势的差值来判断地守在真实攻击实验中的优势是否为可忽略的。本文用事件 Succ 表示敌手正确猜测除了在 Test 询问中所使用的随机比特  $b$ , 用  $\text{Adv}(A, P_i)$  表示敌手 A 在第  $i$  个混合实验中的优势。

实验  $P_0$  此实验模拟在随机预言模型下的真实协议运行。在实验中, 敌手可以多次访问 Execute、Send 和 Text 询问。根据定义有

$$\text{Adv}_P^{\text{AKE}}(A) = \text{Adv}(A, P_0)$$

实验  $P_1$  在这个实验中, 本文通过维持哈希列表来模拟随机预言函数  $h, H$ 。另外还模拟一个私有的随机预言函数  $H'$ , 这几个私有的随机预言函数将在后面的实验中用到。随机预言函数的模拟规则如下:

a)  $h$  查询列表  $hList$ 。对于每一次随机预言询问  $h(m)$ , 如果列表  $hList$  中存在记录  $(m, r)$ , 则返回  $r$ ; 否则, 随机选取  $r \in \{0, 1\}^n$ , 将  $r$  返回给询问者, 并且将记录  $(m, r)$  添加到列表  $hList$  中。

b)  $H$  查询列表  $HList$ 。对于每一次随机预言询问  $H(m)$ , 如果列表  $HList$  中存在记录  $(m, r)$ , 则返回  $r$ ; 否则, 随机选取  $r \in \{0, 1\}^n$ , 将  $r$  返回给询问者, 并且将记录  $(m, r)$  添加到列表  $HList$  中。

c)  $H'$  查询列表  $H'List$ 。对于每一次随机预言询问  $H'(m)$ , 如果列表  $H'List$  中存在记录  $(m, r)$ , 则返回  $r$ ; 否则, 随机选取  $r \in \{0, 1\}^n$ , 将  $r$  返回给询问者, 并且将记录  $(m, r)$  添加到列表  $H'List$  中。

除了模拟的随机预言函数外, 还根据协议描述模拟所有的 Execute、Send 和 Test 询问。由模拟的规则可知:

$$\text{Adv}(A, P_0) = \text{Adv}(A, P_1)$$

实验  $P_2$  在这个实验中本文考虑敌手的被动窃听能力, 修改对 Execute 询问的模拟。如果攻击者 A 能够在此实验中以不可忽略的优势区分随机数和会话密钥, 那么模拟者就可以利用攻击者的能力破坏 Hash 函数。为了利用攻击者的能力, 模拟者模拟整个实验的运行。首先模拟者在网关节点处注册若干个诚实用户和若干个传感器节点, 因此, 模拟者知道每个用户和节点的秘密值(长期私钥及智能卡等)。每当敌手 A 进行 Execute 查询时, 让模拟者在会话进行中, 选取相应的随机数  $N_1, N_2$  和  $N_3$ , 并用按照实验  $P_1$  的规则用模拟的随机预言函数  $H$  计算出相应的消息值如  $K_i, E_i, W_i, V_i, M_i, R_i, F_i, S_i$ 。模拟到最后计算会话密钥时, 利用自己的私有随机预言函数, 令会话密钥  $SK = H'(* \parallel C_i \parallel D_i \parallel E_i \parallel F_i \parallel W_i \parallel V_i)$ 。

首先说明的是模拟者为敌手 A 模拟的协议运行环境除了可忽略的概率外是完美的, 除非是 A 察觉到会话密钥  $SK$  计算有误, 并对其随机预言函数  $H$  列表进行查询。而此时, 一旦敌手 A 对  $HList$  列表进行  $H(K \parallel C_i \parallel D_i \parallel E_i \parallel F_i \parallel W_i \parallel V_i)$  询问, 模拟者便可得到中间秘密值  $K$ 。首先假设  $G$  是一个真正的随机预言函数, 则通过设定以下游戏来说明在模拟者得到中间秘密值  $K$  后, 是如何破坏哈希函数的安全性。

游戏  $G_1$

阶段 1 模拟者向  $G$  挑战  $N_1, N_2, N_3, G$  选择一个随机比特值  $z$ , 当  $z=1$  时, 则  $G$  返回  $K = H((N_1 \oplus N_2 \oplus N_3) \parallel H(\overline{ID}_i \parallel y_i \parallel N_1))$ ; 当  $z=0$  时, 则返回随机值  $s^*$ 。

阶段 2 模拟者可以向  $G$  查询  $N'_1, N'_2, N'_3, G$  返回  $K = H((N'_1 \oplus N'_2 \oplus N'_3) \parallel H(\overline{ID}_i \parallel y'_i \parallel N'_1))$ , 模拟者可以重复多次不同的  $N'_1, N'_2, N'_3$ 。

阶段 3 模拟者输出  $z'$  作为对  $z$  的猜测, 当  $z'=z$  时, 则称模拟者赢得了这场游戏。

假设模拟者利用敌手 A 的能力得到了中间秘密值  $K$ , 则模

拟者可以轻易地指出上述游戏中  $G$  回答的是  $K = H((N_1 \oplus N_2 \oplus N_3) \parallel H(\overline{ID}_i \parallel y_i \parallel N_1))$  还是一个随机值  $s^*$ , 即模拟者以不可忽略的概率猜测出了  $z' = z$ , 赢得了这场游戏。因此, 当敌手  $A$  以不可忽略的概率成功区分一个随机值和会话密钥时, 模拟者便可以不可忽略的概率区分一个 hash 值和一个随机值(在未输入  $y_i$  的前提下), 那么哈希函数  $H$  就被破坏了, 这违背了假设。因此敌手赢得此实验的概率是可忽略的, 即

$$|\text{Adv}(A, P_1) - \text{Adv}(A, P_2)| \leq \text{neg}(l)$$

实验  $P_3$  从这个实验开始, 本文考虑敌手的主动攻击能力。在攻击有意义的前提下, 假设敌手是不能腐化网关节点  $GW$  的。认为敌手  $A$  如果没有同时进行对用户  $U_i$  作  $\text{CorruptLL}(U_i)$  和  $\text{CorruptSC}(U_i)$  查询, 那么  $A$  就不能仿冒用户, 即不能伪造出第一条发送的消息  $\{\overline{ID}_i, C_i, K_i\}$ 。假设  $A$  在没有完全腐化用户的前提下, 成功仿冒用户伪造了消息  $\{\overline{ID}_i, C_i, K_i\}$ , 则认为敌手  $A$  攻击成功, 则模拟失败, 实验终止。把敌手攻击成功的事件分以下两种情况:

情况 1 敌手  $A$  对用户做出  $\text{CorruptLL}(U_i)$  查询, 但没有做出  $\text{CorruptSC}(U_i)$  查询。在这种情况下, 如果敌手成功伪造出消息  $\{\overline{ID}_i, C_i, K_i\}$ , 其中  $C_i = H(x) \oplus y_i \oplus N_1, K_i = H(H(x) \parallel y_i \parallel N_1 \parallel \overline{ID}_i)$ , 则称敌手攻击成功。本文先排除一些发生碰撞的会话, 具体来说, 如果消息抄本  $\{\overline{ID}_i, C_i, K_i\}$  发生碰撞, 或者随机预言函数的输出发生碰撞, 那么敌手赢得了实验, 取消该次会话的运行。由生日攻击原理可知, 发生碰撞的概率为  $q_s/2^k$ 。其中:  $q_s$  为这个实验中产生实例数的上界,  $k$  为安全参数。即发生碰撞的概率是可忽略的。因此, 得知敌手已获取秘密值  $H(x)、y_i$  和  $N_1$ , 从而成功伪造出消息  $\{\overline{ID}_i, C_i, K_i\}$ 。通过此情况的设定, 敌手在未知智能卡中存储秘密值的条件下,  $A$  只能通过用户的口令  $PW$  以及以前会话中消息  $\overline{ID}_i, C'_i, K'_i$  获取相关信息。在方案中,  $y_i = G_i \oplus \overline{ID}_i \oplus \overline{PW}_i, H(x) = H_i \oplus \overline{PW}_i \oplus H(y_i)$ , 在没有获取智能卡的条件下敌手无法直接计算  $H(x)、y_i$  和  $N_1$ 。根据随机预言机的真随机性, 敌手要么直接对其值进行猜测, 概率为  $1/2^k$ , 要么对模拟随机预言函数  $H$  进行查询从而猜测, 其概率为  $q_h N \times \varepsilon$ 。由此可知, 在情况 1 的条件下, 敌手攻击成功的概率是可忽略的。

情况 2 敌手  $A$  对用户作出  $\text{CorruptSC}(U_i)$  查询, 但没有做出  $\text{CorruptLL}(U_i)$  查询。在这种情况下, 如果敌手成功伪造出消息  $\{\overline{ID}_i, C_i, K_i\}$ , 则称敌手攻击成功。同理情况 1, 本文先排除一些发生碰撞的会话, 由生日攻击原理得其概率为  $q_s/2^k$  是可忽略的。而在方案中,  $y_i = G_i \oplus \overline{ID}_i \oplus \overline{PW}_i, H(x) = H_i \oplus \overline{PW}_i \oplus H(y_i)$ ,  $A$  在无法获取口令  $PW$  的前提下无法直接计算  $H(x)、y_i$  和  $N_1$ , 根据随机预言机的真随机性, 敌手要么直接对其值进行猜测, 概率为  $1/2^k$ , 要么对模拟随机预言函数  $H$  进行查询从而猜测, 其概率为  $q_h N \times \varepsilon$ 。由此可知, 同样在情况 2 的条件下, 敌手攻击成功的概率是可忽略的。

综上情况分析, 敌手  $A$  赢得此实验的概率是可忽略的, 即

$$|\text{Adv}(A, P_2) - \text{Adv}(A, P_3)| \leq q_s/2^k + 1/2^k + q_h N \times \varepsilon$$

实验  $P_4$  这个实验中, 本文仍然考虑敌手的主动攻击能力, 认为敌手  $A$  如果没有进行对传感器节点作出  $\text{CorruptLL}(S_i)$ , 那么  $A$  就不能伪造出消息  $\{\overline{ID}_i, C_i, K_i, SID_s, D_i, E_i\}$ 。假设  $A$  在没有腐化传感器节点  $S_i$  的前提下, 成功仿冒用户伪造

了消息  $\{\overline{ID}_i, C_i, K_i, SID_s, D_i, E_i\}$ , 则认为敌手  $A$  攻击成功, 则模拟失败, 实验终止。

本文仍然通过设定一个游戏来说明。假如敌手  $A$  能伪造出消息  $\{\overline{ID}_i, C_i, K_i, SID_s, D_i, E_i\}$ , 则敌手可破坏哈希函数的安全性。

### 游戏 $G_2$

阶段 1 敌手  $A$  向  $G$  挑战  $C_i, K_i, D_i, G$  选择一个随机比特值  $z$ , 当  $z=1$  时, 则  $G$  返回  $E_i = H(\overline{ID}_i \parallel C_i \parallel K_i \parallel D_i \parallel SID_s \parallel h(x \parallel SID_s))$ ; 当  $z=0$  时, 则返回随机值  $s^*$ 。

阶段 2 敌手  $A$  可以向  $G$  查询  $C'_i, K'_i, D'_i, G$  返回  $E_i = H(\overline{ID}_i \parallel C'_i \parallel K'_i \parallel D'_i \parallel SID_s \parallel h(x \parallel SID_s))$ , 敌手  $A$  可以重复多次不同的  $C'_i, K'_i, D'_i$ 。

阶段 3 敌手  $A$  输出  $z'$  作为对  $z$  的猜测, 当  $z'=z$  时, 则称敌手  $A$  赢得了这场游戏。

假设敌手  $A$  伪造出消息合法的消息  $\{\overline{ID}_i, C_i, K_i, SID_s, D_i, E_i\}$ , 则敌手  $A$  可以轻易地指出上述游戏  $G_2$  中  $G$  回答的是  $E_i = H(\overline{ID}_i \parallel C_i \parallel K_i \parallel D_i \parallel SID_s \parallel h(x \parallel SID_s))$  还是一个随机值  $s^*$ , 即敌手  $A$  以不可忽略的概率猜测出了  $z' = z$ , 赢得了这场游戏。因此, 当敌手  $A$  以不可忽略的概率成功伪造出合法消息仿冒传感器节点时, 敌手  $A$  便可以不可忽略的概率区分一个 Hash 值和一个随机值(在未知输入值  $h(x \parallel SID_s)$  的前提下), 那么哈希函数  $H$  就被破坏了, 这违背了假设。因此敌手赢得此实验的概率是可忽略的, 即

$$|\text{Adv}(A, P_3) - \text{Adv}(A, P_4)| \leq \text{neg}(l)$$

实验  $P_5$  这个实验中, 同理实验  $P_4$ , 由于本文认为敌手  $A$  在攻击有意义的前提下不允许腐化网关节点  $GW$ , 那么如果没有进行对传感器节点作出  $\text{CorruptLL}(S_i)$ , 则  $A$  就不能伪造出消息  $\{W_i, V_i, M_i, R_i, F_i\}$ 。假设  $A$  在没有腐化传感器节点  $S_i$  的前提下, 成功仿冒用户伪造了消息  $\{W_i, V_i, M_i, R_i, F_i\}$ , 则认为敌手  $A$  攻击成功, 则模拟失败, 实验终止。同理上一个实验  $P_4$  的证明, 假如当敌手  $A$  以不可忽略的概率成功伪造出合法消息仿冒网关节点时, 敌手  $A$  便可以不可忽略的概率区分一个 Hash 值和一个随机值(在未知输入值  $h(x \parallel SID_s)$  的前提下), 那么哈希函数  $H$  就被破坏了, 这违背了假设。因此敌手赢得此实验的概率是可忽略的, 即

$$|\text{Adv}(A, P_4) - \text{Adv}(A, P_5)| \leq \text{neg}(l)$$

实验  $P_6$  这个实验中, 在攻击有意义的前提下, 假设敌手是不能腐化网关节点  $GW$  的。本文认为敌手  $A$  如果没有同时进行对用户  $U_i$  作  $\text{CorruptLL}(U_i)$  和  $\text{CorruptSC}(U_i)$  查询, 那么  $A$  就不能仿冒网关节点去欺骗用户, 即不能伪造出第一条发送的消息  $\{W_i, V_i, S_i\}$ 。假设  $A$  在没有完全腐化用户的前提下, 成功仿冒网关节点伪造了消息  $\{W_i, V_i, S_i\}$ , 则认为敌手  $A$  攻击成功, 则模拟失败, 实验终止。同理实验  $P_3$ , 也可分两种情况, 显然最后得出敌手赢得此实验的概率是可忽略的, 即

$$|\text{Adv}(A, P_5) - \text{Adv}(A, P_6)| \leq q_s/2^k + 1/2^k + q_h N \times \varepsilon$$

模拟到最后, 所有的被动会话的会话密钥都是随机选择的, 而敌手进行主动攻击的会话都会被拒绝接受, 但目前为止模拟仍然没有终止, 即攻击者  $A$  未伪造成功。根据上面的分析可知, 敌手在区分真实的会话密钥和随机数不会有任何优势, 因此  $\Pr[\text{Succ}] = 1/2$ 。最后综合上面所有等式的结果定理 1 得证。

附录中表 1 给出了新提出的方案与现存的无线传感器网络下双因素用户认证密钥交换协议在安全性上的对比。其中,

PIA 表示特权内部人攻击<sup>[2~4]</sup>, UIA 表示用户仿冒攻击<sup>[11]</sup>, GA 表示猜测攻击<sup>[2,5,6]</sup>, NCA 表示节点捕获攻击<sup>[4~8]</sup>, GIA 表示网关仿冒攻击<sup>[11]</sup>, SRA 表示智能卡泄露攻击<sup>[4]</sup>, PA 表示平行会话攻击<sup>[10,12]</sup>, SK 表示该方案有会话密钥的建立; Y 表示该方案能抵抗此攻击, N 表示该方案不能抵抗此攻击。

## 5.2 性能分析

在这一小节本文将主要对新方案的在注册阶段和登录/认证阶段的计算效率和通信效率进行分析,其与相关方案的性能比较如附录中表 2 所示。其中, H 表示单向哈希函数操作, Pub/Pri 表示公/私钥密码函数操作, Se/Sd 表示对称密码加/解密操作, MAC 表示消息认证码函数操作, PM/PA 表示椭圆曲线点乘/加计算操作, E 表示椭圆曲线多项式计算操作。

计算效率:在注册阶段,主要考虑计算效率,提出的新方案中用户和网关节点分别只需要 5 和 2 个哈希函数操作。在登录和认证阶段,用户、网关节点和传感器节点分别只需要 12、10 和 7 个哈希函数操作。虽然与 Kalra 的方案相比多了几个哈希函数操作,但是与 Yuan<sup>[9]</sup>、Yeh<sup>[16]</sup> 以及 RUASN<sup>[15]</sup> 方案相比,本文提出的方案在保证安全性的前提下不需要(非)对称密码操作和 MAC 等复杂的计算量,因此更适合资源受限的无线传感器网络环境。

通信效率:在无线传感器网络环境下,资源受限的传感器节点并没有持续的电源供应,而其最耗能的是通信模块,主要包括接收、发送消息等。因此,方案中交换的消息数量(轮数)至关重要。本文新提出的方案在满足所有安全性能的前提下,只需要四轮来进行消息交换。而在同样轮数或仅需更少轮数的其他方案中,都存在多种安全缺陷。显然,新方案更适合资源受限的无线传感器网络环境。

综上所述,考虑计算效率和通信效率的情况下,新方案是一个高效安全且更适合实际应用需求的方案。

## 6 结束语

本文对 Kalra 的方案进行了回顾,并对其进行了安全性的分析,发现其方案存在许多致命的安全缺陷,如存在节点仿冒攻击导致未达到双向认证、由智能卡丢失引起的密钥泄露从而未满足前向安全性、存在用户仿冒攻击等。基于 Kalra 方案的安全漏洞对其进行改进,提出了一个可证安全的双因素用户认证密钥协商方案。该方案针对资源受限的无线传感器网络环境以及现实应用中敌手的能力,不仅保证了用户的匿名性,还达到了用户、网关节点、传感器节点三者之间的双向认证,可以抵抗多种已知攻击,特别是智能卡泄露攻击,并且建立了具有前向安全性的会话密钥。本文给出了新方案在 Nam 提出的首个针对无线传感器网络中双因素认证方案安全模型中的安全性证明,最后与其他现存方案在安全性和效率上进行了相比,提出的新方案拥有更高的安全性,且计算量小、通信成本低、更高效,适合资源受限环境及现实应用。然而针对无线传感器网络方向下的双因素用户认证密钥协商方案, Nam 的安全模型仍然需要完善,提出一个更适当的安全模型并对此类方案进行更严谨的安全性证明仍是未来进一步需要完成的工作。

## 参考文献:

- [1] Das M L. Two-factor user authentication in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2009, 8 (3): 1086-1090.
- [2] He Daojing, Gao Yi, Chan S, et al. An enhanced two-factor user authentication scheme in wireless sensor networks[J]. Ad Hoc & Sensor Wireless Networks, 2010, 10(4): 361-371.
- [3] Khan M K, Alghathbar K. Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks’[J]. Sensors, 2010, 10(3): 2450-2459.
- [4] Sun Dazhi, Li Jianxin, Feng Zhiyong, et al. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks[J]. Personal and Ubiquitous Computing, 2013, 17 (5): 895-905.
- [5] Nyang D H, Lee M K. Improvement of das’s two-factor authentication protocol in wireless sensor networks[Z]. IACR Cryptology ePrint Archive. 2009: 631.
- [6] Huang Hufeng, Chang Yafen, Liu C H. Enhancement of two-factor user authentication in wireless sensor networks[C]//Proc of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2010: 27-30.
- [7] Kumar P, Lee H J. Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks[C]//Proc of Wireless Advanced. 2011: 241-245.
- [9] Yuan Jianjun. An enhanced two-factor user authentication in wireless sensor networks[J]. Telecommunication Systems, 2014, 55(1): 105-113.
- [8] Vaidya B, Makrakis D, Mouftah H T. Improved two-factor user authentication in wireless sensor networks[C]//Proc of the 6th International Conference on Wireless and Mobile Computing, Networking and Communications. 2010: 600-606.
- [10] Chen T H, Shih W K. A robust mutual authentication protocol for wireless sensor networks[J]. Etri Journal, 2010, 32(5): 704-712.
- [11] Li Chunta, Lee C C, Wang Lianjun, et al. A secure billing service with two-factor user authentication in wireless sensor networks[J]. International Journal of Innovative Computing, Information and Control, 2011, 7(8): 4821-4832.
- [12] Yoo S G, Park K Y, Kim J. A security-performance-balanced user authentication scheme for wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2012, 2012:1-11.
- [13] Fan Rong, Ping Lingdi, Fu Jianqing, et al. A secure and efficient user authentication protocol for two-tiered wireless sensor networks [C]//Proc of the 2nd Pacific-Asia Conference on Circuits, Communications and System. 2010: 425-428.
- [14] Fan Rong, He Daojing, Pan Xuezeng, et al. An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks[J]. Journal of Zhejiang University: Science C, 2011, 12 (7): 550-560.
- [15] Kumar P, Choudhury A J, Sain M, et al. RUASN: a robust user authentication framework for wireless sensor networks [J]. Sensors, 2011, 11(5): 5020-5046.
- [16] Yeh H L, Chen T H, Liu Pinchuan, et al. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography [J]. Sensors, 2011, 11(5): 4767-4779.
- [17] Shi Wenbo, Gong Peng. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography [J]. International Journal of Distributed Sensor Networks, 2013, 2013:1-7.
- [18] Xue Kaiping, Ma Changsha, Hong Peilin, et al. A temporal-creden-

- tial-based mutual authentication and key agreement scheme for wireless sensor networks [J]. *Journal of Network and Computer Applications*, 2013, 36(1): 316-323.
- [19] Kalra S, Sood S K. Advanced password based authentication scheme for wireless sensor networks [J]. *Journal of Information Security and Applications*, 2015, 20: 37-46
- [20] Nam J, Kim M, Paik J, et al. A provably-secure ECC-based authentication scheme for wireless sensor networks [J]. *Sensors*, 2014, 14(11): 21023-21044.
- [21] Li Xinghua, Bao Fenye, Li S, et al. FLAP: an efficient WLAN initial access authentication protocol [J]. *IEEE Trans on Parallel and Distributed Systems*, 2014, 25(2): 488-497.

附录:

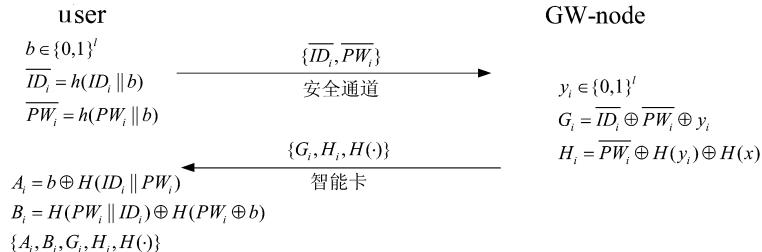


图 1 新方案的注册阶段

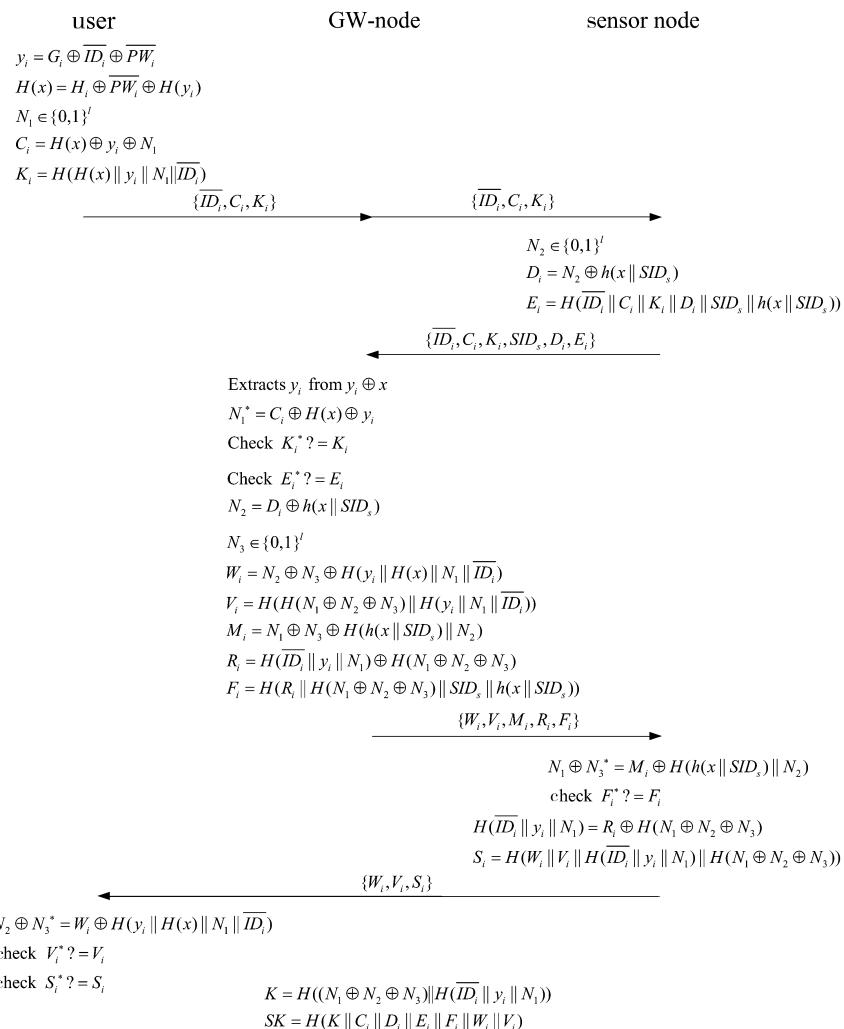


图 2 新方案的登录、认证及会话密钥建立阶段

(下转第 页)

(上接第 页)

表 1 新方案与同类方案的安全性对比

方案/攻击	PIA	UIA	GA	NCA	GIA	SRA	PA	SK
Das' [1]	N	N	N	N	N	N	N	N
Nyang-lee[5]	N	N	N	N	N	N	N	Y
He's[2]	Y	N	N	N	N	N	N	N
Huang's[6]	N	N	N	Y	N	N	N	N
K-A[3]	N	N	N	N	N	N	N	N
Sun's[4]	Y	Y	N	Y	Y	N	Y	N
Yuan's[9]	N	N	N	N	N	N	Y	N
Vaida's[8]	N	N	N	N	N	N	N	N
Chen-shih[10]	N	N	N	N	N	N	N	N
Li et al.'s[11]	N	Y	Y	N	Y	N	Y	N
Yoo's[12]	Y	N	N	Y	Y	N	Y	N
Ruasn[15]	N	N	N	Y	Y	N	Y	Y
Yeh's[16]	Y	N	N	Y	Y	N	Y	Y
Shi's[17]	Y	N	N	Y	Y	N	Y	Y
Kalra's[19]	Y	N	N	Y	Y	N	Y	Y
新方案	Y	Y	Y	Y	Y	Y	Y	Y

表 2 新方案与同类方案的性能对比

方案/阶段	注册阶段		登陆/认证阶段			轮数
	用户	网关节点	用户	网关节点	传感器节点	
Das' [1]		3H	4H	4H	H	2
Nyang-lee[5]		3H	H + Sd	9H + Se	2H + Se + Sd	3
He's[2]	H	5H	5H	5H	H	2
Huang's[6]		4H	4H	6H	H	2
K-A[3]	H	2H	4H	5H	2H	3
Sun's[4]		2H	2H	5H	2H	5
Yuan's[9]		5H	7H + Pub	7H + Pri	2H	4
Vaida's[8]	H	4H	6H	5H	2H	3
Chen-shih[10]		3H	5H	5H	H	4
Ruasn[15]	H	3H + Se	4H + Se + Sd	4H + Se + Sd + MAC	H + Se + Sd + MAC	4
Yeh's[16]	H	3H + PM	4H + PA + 2PM	4H + 2PA + 3PM + E	3H + PA + PM + E	3
Shi's[17]	H	2H + PM	5H + 3PM	4H + PM	3H + 2PM	4
Kalra's[19]	2H	2H	11H	9H	4H	4
新方案	5H	2H	12H	10H	7H	4