无线传感器网络中身份认证与密钥共识方案

王 牧,亢保元,景东亚
(天津工业大学 计算机科学与软件学院,天津 300387)

摘 要:随着无线通信技术的飞速发展,无线传感器网络(WSN)已经在军事、环境检测、工业以及医疗等领域得到广泛应用,且逐渐成为最有潜力的技术之一。然而,因为无线传感器网络是通过无线信道传送信息,传感器节点通常是部署在无人看管的环境中并且受到计算能力和能量的限制,所以无线传感器网络比起传统网络更容易受到各种各样的攻击。最近 Sheetal Kalra 提出一种无线传感器网络中基于口令的认证方案,并声称这个方案可以抵抗各种攻击。但是,Sheetal Kalra 的方案容易受到来自用户的假冒攻击。文中提出了一种安全高效的基于口令的身份认证与密钥共识方案,并给出了安全性分析,以此证明该方案可以满足无线传感器网络中的安全需求。

关键词:身份认证;密钥共识;传感器网络;安全性
中图分类号:TP918 **文献标识码**:A **文章编号**:1673-629X(2017)12-0098-05
doi:10.3969/j.issn.1673-629X.2017.12.022

An Identity Authentication and Key Agreement Scheme for Wireless Sensor Network

WANG Mu,KANG Bao-yuan,JING Dong-ya
(School of Computer Science and Software Engineering,Tianjin Polytechnic University,
Tianjin 300387,China)

Abstract:With rapid development of wireless communication technology,Wireless Sensor Network (WSN),as one of most gradually potential technologies,can be widely used in various fields such as military,environmental detection,industrial control,and medical monitoring. However,WSN is vulnerable to various attacks than traditional ones because it transmits data by using a wireless channel,and the sensors are commonly deployed in unattended environment and limited with computational and the energy resources. Recently,Sheetal Kalra proposed an advanced password based authentication scheme for wireless sensor network and claimed that it is secure against various type of security attacks. But it is subjected to impersonation attack from the users. For this,a password-based authentication and key agreement scheme for wireless sensor network is proposed. Through security analysis,it is proved that the proposed scheme is more suitable for providing security for various applications in WSN.

Key words:identity authentication;key agreement;wireless sensor network;security

1 概 述

无线传感器网络(WSN)是由大量细小的传感器构成的无线网络,协作地感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息,并最终把这些信息发送给网络的所有者。无线传感器网络通常带有敏感的数据工作在不安全的环境中,因此传感器网络的安全性是无线传感器网络应用的首要问题。在传统的无线传感器网络中,网关节点(GWN)通常用来连接外部的传感器与用户。传感器、用户以及网关之间的通信必须在安全的认证协议保障下才可以进行。用户、网关、传感器之间必须通过相互的认证并达成共享的密钥之后才可以进行通信。

典型的传感器节点通常很小,感应、通信和计算能力均受到所携带电量的限制,减少传感器的能量损耗可以延长传感器的生命周期。因为无线传感器网络的工作受到计算能力和电量的限制,所以传统的网络安全协议不能直接应用在无线传感器网络中。因此,设计出安全高效、低损耗的无线传感器网络认证协议是面临的一项重要挑战。

近年来,很多身份认证和密钥共识方案相继提出。

收稿日期:2016-08-12 **修回日期**:2016-12-21 **网络出版时间**:2017-09-27
基金项目:天津市应用基础与前沿技术研究计划(15JCYBJC15900)
作者简介:王 牧(1990-),男,硕士研究生,研究方向为信息安全;亢保元,博士,教授,研究方向为信息安全。

2004 年,Watro 等[1]提出了基于公钥加密的方案,但该方案计算量大、效率低;2009 年,Das[2]指出 Watro 的方案不能抵抗假冒攻击和重放攻击,并提出了包含网关节点的无线传感器网络的双方认证方案。尽管这个方案是高效的,但是不能提供相互认证和共享密钥;2010 年,He 等[3]和 Khan 等[4]分别改进了 Das 的方案。改进方案在网关节点和传感器节点之间利用口令的哈希值而不是直接利用口令进行相互认证,但是这个方案中网关节点的存储空间受到限制,并且口令更新阶段难以实现。2010 年,Chen 等[5]提出了用户、网关节点、传感器节点间的认证方案,但是这个方案容易受到伪造攻击和重放攻击;2011 年,Yeh 等[6]提出了基于 ECC 的远程认证方案,该方案与其他方案相比计算量大很多;2013 年,He 等[7]提出了移动设备中的口令认证方案;2015 年,He 等[8]提出了基于临时证书的匿名认证方案。

2013 年,Xue 等[9]提出了基于临时证书的相互认证和密钥共识方案,该方案提供了用户、网关节点、传感器节点之间的相互认证和共享密钥。2015 年,Sheetal Kalra[10]指出 Xue 的方案不能抵抗假冒攻击和智能卡丢失攻击等,并提出了高效的无线传感器网络中基于口令的认证方案。然而 Sheetal Kalra 提出的方案不能抵抗因数据库泄露和智能卡丢失而产生的假冒攻击[11],此外,方案不能达成正确的共享密钥。

2015 年,Sheetal Kalra 提出了基于口令的无线传感器网络认证方案,该方案提供了用户、传感器、网关节点之间的相互认证并达成了共享密钥。文中分析了 Sheetal Kalra 提出的方案,发现这个方案容易在数据库泄露和用户智能卡丢失的情况下受到用户的假冒攻击,并且不能达成正确的共享密钥。

因此,文中提出了一种改进的带有智能卡的认证方案,解决了 Sheetal Kalra 方案中的安全性问题并且达成了正确的共享密钥[12]。此外,还给出了新方案的安全性分析,以此证明该方案可以满足无线传感器网络中的安全需求。

2　Sheetal Kalra 方案

2015 年,Sheetal Kalra 提出了高效的无线传感器网络中基于口令的认证方案。在这个方案中,假设攻击者不可以拦截到通过安全信道传送的信息,攻击者可以拦截到通过无线公共信道传送的信息,并有能力更改、删除、转发这些信息,如果用户的智能卡丢失,攻击者可以提取出智能卡中的数据[13]。该方案包括四个阶段:注册阶段,登录阶段,认证和密钥共识阶段,口令改变阶段。

相关参数见表 1。

表 1　相关参数

参数	意义	参数	意义
U_i	第 i 个用户	$H(\cdot)$	单向哈希函数
GWN	网关节点	y_i	网关节点为第 i 个用户选取的随机数
S_S	第 S 个传感器节点	X	网关节点的私钥
SID_S	第 S 个传感器节点的身份地址	N_1	由用户的智能卡生成的随机数
SK_S	第 S 个传感器节点的私钥	N_2	由传感器节点生成的随机数
SK	达成的共享密钥	N_3	由网关节点生成的随机数
ID_i	第 i 个用户的身份地址	$\oplus$	模二加法运算
P_i	第 i 个用户的口令	$\|$	级联操作

3　安全性分析

Sheetal Kalra 声称他们的方案可以抵抗各种各样的攻击,通过仔细分析,笔者发现这个方案不能抵抗数据库泄露攻击和智能卡丢失攻击。此外,该方案中用户、传感器节点、网关节点之间并不能得到共享密钥[14],详细分析如下。

3.1　数据库泄露攻击

假设有一个恶意的用户 U_k 拥有一个智能卡并提取出智能卡里的信息 $(A_k,B_k,G_k,H_k,H(\cdot))$,$U_k$ 利用自己的 ID_k 口令 P_k 和这些提取出的信息,就可以计算 $n_k=A_k\oplus H(\mathrm{ID}_k\|P_k)$,$E_k=H(\mathrm{ID}_k\|n_k)$,$F_k=H(n_k\oplus P_k)$,$y_k=G_k\oplus E_k$,$H(x)=H_k\oplus F_k\oplus H(y_k)$,所以可以得到 y_k,$H(x)$。如果网关节点的数据库中存储的数据 J_i 和 $y_i\oplus x$ 泄露给 U_k,这个恶意用户就可以根据 J_k 和 $y_k\oplus x$ 得到 x,并可以得到任一用户 U_i 的信息 y_i,$J_i,E_i=J_i\oplus H(y_i)\oplus x$。利用这些数据,$U_k$ 就可以伪造用户 U_i 的登录信息。首先,U_k 生成一个随机数 N_1',计算 $\mathrm{CID}_i'=E_i\oplus H(y_i)\oplus H(x)\oplus N_1'$,$C_i'=H^2(x)\oplus N_1'$,$K_i'=H(H(x)\|y_i\|N_1')$。于是 U_k 把 $(C_i',\mathrm{CID}_i',K_i')$ 发给网关节点,网关节点根据 SID_S 把收到的请求转发给附近的传感器节点。传感器节点收到 $(C_i',\mathrm{CID}_i',K_i')$ 之后生成随机数 N_2,并计算 $D_i=N_2\oplus\mathrm{SK}_S$,然后把请求消息 $(\mathrm{SID}_S,C_i',\mathrm{CID}_i',K_i',D_i)$ 发给网关节点。网关节点从 $\mathrm{SK}_S\oplus H(x\|\mathrm{SID}_S)$ 中提取出 SK_S,并计算 $N_1'=C_i'\oplus H^2(x)$,$N_2=D_i\oplus\mathrm{SK}_S$,$J_i^*=\mathrm{CID}_i'\oplus N_1'\oplus H(x)\oplus x=J_i$,网关节点在数据库中根据 J_i^* 从 $y_i\oplus x$ 中提取出 y_i。网关节点又计算 $K_i^*=H(H(x)\|y_i\|N_1')=K_i'$,可以通过验证,所以网关节点接受这个登录请求。

综上所述,如果网关节点的数据库泄露,一个恶意的用户 U_k 能够得到 x 和 y_i,而且可以进行用户假冒攻击。

3.2 智能卡丢失攻击

在 Sheetal Kalra 的方案中,声称即使是智能卡丢失,这个方案也是安全的,然而事实却不是这样。就像上述的数据库泄露攻击中,一个恶意的用户 U_k 拥有自己的智能卡,并且能提取出智能卡中的内容 $(A_k, B_k, G_k, H_k, H(\cdot))$,经过计算得到 $H(x)$。如果 U_k 截获了某个合法用户 U_i 的登录信息 $(\mathrm{CID}_i, C_i, K_i)$,$U_k$ 就可以计算 $N_1 = C_i \oplus H^2(x)$,$E_i \oplus H(y_i) = \mathrm{CID}_i \oplus H(x) \oplus N_1$。如果这个合法用户 U_i 的智能卡被 U_k 盗取,U_k 就可以提取出其中的 $(A_i, B_i, G_i, H_i, H(\cdot))$,然后计算 $n \oplus P_i = A_i \oplus B_i$,$H(n \oplus P_i) = F_i$,$H(y_i) = H_i \oplus F_i \oplus x$,所以 U_k 就可以得到 $E_i = H(y_i) \oplus (E_i \oplus H(y_i))$,$y_i = G_i \oplus E_i$。利用 $H(x)$,y_i,E_i,这个恶意用户 U_k 就可以伪造出 $(C_i', \mathrm{CID}_i', K_i')$,并把 $(C_i', \mathrm{CID}_i', K_i')$ 发给网关节点进行用户假冒攻击,所以 Sheetal Kalra 的方案并不能像他们所声称的那样能抵抗智能卡丢失攻击。

3.3 错误的共享密钥

在注册阶段,用户 U_i 向网关节点提交了 E_i, F_i 而不真正的 ID_i,网关节点也没有储存真正的 ID_i。在登录阶段为了实现匿名性,智能卡发送匿名身份 $\mathrm{CID}_i = E_i \oplus H(y_i) \oplus H(x) \oplus N_1$ 而不是用户的真正身份信息 ID_i,所以在登录及认证阶段都没有用户的真正身份信息 ID_i。也就是说,传感器节点和网关节点都不可能得到用户 U_i 的身份信息 ID_i,然而生成的共享密钥 $\mathrm{SK} = H(H(\mathrm{ID}_i \| y_i \| N_1) \| (N_1 \| N_2 \| N_3))$ 中却包含了 ID_i,所以认为得到的这个共享密钥是错误的。

4 改进方案

文中提出了一种安全高效的方案(见图 1),以解决 Sheetal Kalra 方案中的问题。该方案同样包括三个参与者,用户 U_i、传感器节点 S_j、网关节点 GWN。网关节点选取一个大素数 p,g 是 Z_p^* 的生成元,选取私钥 $x \in Z_{p-1}^*$,公钥 $y_{\mathrm{GWN}} = g^x \bmod p$。

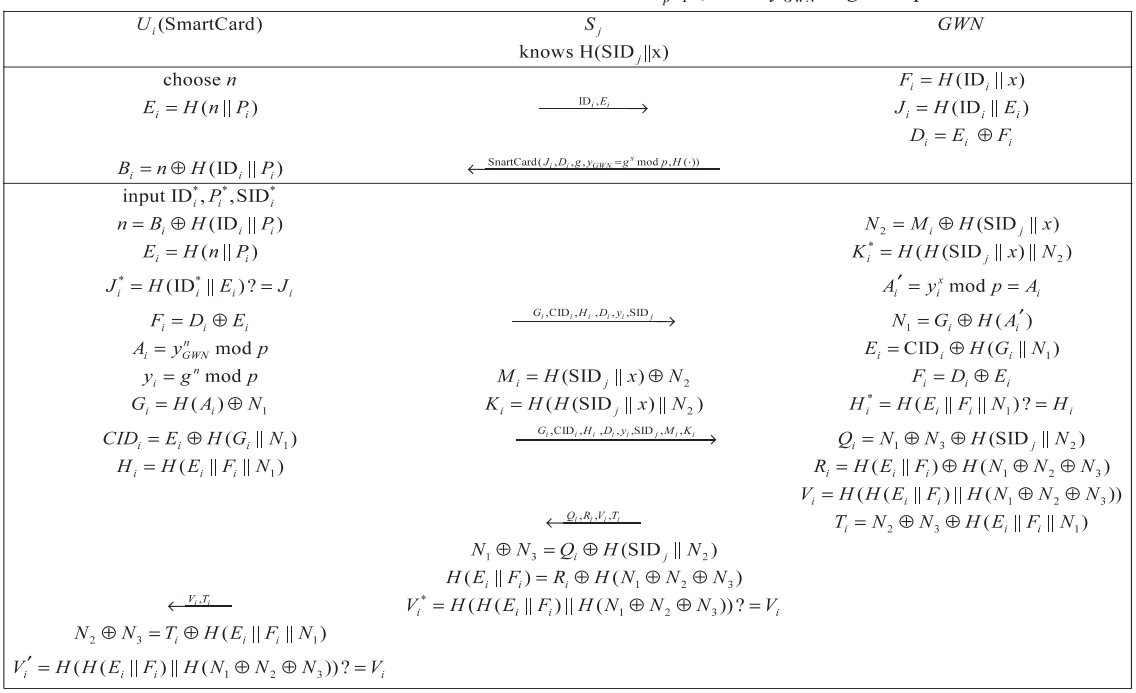

图 1 文中方案

4.1 注册阶段

用户 U_i 首先要向网关节点进行注册,注册阶段都是在安全信道中进行的。

用户 U_i 选取一个随机数 n,计算 $E_i = H(n \| P_i)$,然后把 ID_i, E_i 通过安全信道提交给网关节点。

Step1: $U_i \rightarrow \mathrm{GWN}: \mathrm{ID}_i, E_i$

网关节点收到 ID_i, E_i 之后,计算 $F_i = H(\mathrm{ID}_i \| x)$,$J_i = H(\mathrm{ID}_i \| E_i)$,$D_i = E_i \oplus F_i$,网关节点把 $(J_i, D_i, g, y_{\mathrm{GWN}}, H(\cdot))$ 存储在智能卡中并把智能卡通过安全信道颁发给用户。

Step2: $\mathrm{GWN} \rightarrow U_i$: SmartCard

当用户收到智能卡之后,计算 $B_i = n \oplus H(\mathrm{ID}_i \| P_i)$,并把 B_i 保存在智能卡中,最终智能卡存储了 $(J_i, D_i, B_i, g, y_{\mathrm{GWN}}, H(\cdot))$。

每一个传感器节点也要在网关节点进行注册。当传感器节点用它的身份 SID_j 向网关节点注册时,网关节点计算 $H(\mathrm{SID}_j \| x)$,然后把 $H(SID_j \| x)$ 提交给传感器节点保存。

4.2 登录阶段

用户 U_i 把智能卡插入读卡器中并输入 ID_i^* 和口

令 P_i^* 以及传感器节点身份 SID_j,智能卡计算 $n = B_i \oplus H(\mathrm{ID}_i \| P_i)$,$E_i = H(n \| P_i)$,$J_i^* = H(\mathrm{ID}_i \| E_i)$,并验证 $J_i^* ? = J_i$,如果上式成立,就说明 U_i 是一个合法用户。

Step1: SmartCard checks $J_i^* ? = J_i$

验证成功后,智能卡生成一个随机数 N_1,并计算 $F_i = D_i \oplus E_i$,$A_i = y_{\mathrm{GWN}}^n \mathrm{mod} p$,$y_i = g^n \mathrm{mod} p$,$G_i = H(A_i) \oplus N_1$,$\mathrm{CID}_i = E_i \oplus H(G_i \| N_1)$,$H_i = H(F_i \| E_i \| N_1)$,于是智能卡把登录请求 $(G_i, H_i, D_i, y_i, \mathrm{CID}_i)$ 通过公共信道发送给网关节点。

Step2: SmartCard → GWN: $G_i, H_i, D_i, y_i, \mathrm{CID}_i, \mathrm{SID}_j$

网关节点根据传感器身份 SID_j,把收到的请求转发给附近的传感器节点。

4.3　认证和密钥共识阶段

收到网关节点发来的登录请求之后,传感器节点选取一个随机数 N_2,计算 $M_i = H(\mathrm{SID}_j \| x) \oplus N_2$,$K_i = H(H(\mathrm{SID}_j \| x) \| N_2)$,之后传感器节点把登录请求 $(G_i, H_i, D_i, y_i, \mathrm{CID}_i, \mathrm{SID}_j, M_i, K_i)$ 发送给网关节点。

Step1: S_S → GWN: $G_i, H_i, D_i, y_i, \mathrm{CID}_i, \mathrm{SID}_j, M_i, K_i$

当收到登录请求 $(G_i, H_i, D_i, y_i, \mathrm{CID}_i, \mathrm{SID}_j, M_i, K_i)$ 后,网关节点开始计算 $N_2 = M_i \oplus H(\mathrm{SID}_j \| x)$,$K_i^* = H(H(\mathrm{SID}_j \| x) \| N_2)$,并且验证 K_i^* 是否等于 K_i,如果验证等式成立,网关节点认为传感器节点的身份合法,否则拒绝这次请求。

Step2: GWN checks $K_i^* ? = K_i$

网关节点计算 $A_i' = y_i^x \mathrm{mod} p = A_i$,$N_1 = G_i \oplus H(A_i')$,$E_i = \mathrm{CID}_i \oplus H(G_i \| N_1)$,$F_i = D_i \oplus E_i$,$H_i^* = H(E_i \| F_i \| N_1)$,验证 H_i^* 是否等于 H_i,如果等式成立,网关节点认为用户的身份合法,否则网关节点拒绝这次请求。

Step3: GWN checks $H_i^* ? = H_i$

网关节点生成一个随机数 N_3,计算 $Q_i = N_1 \oplus N_3 \oplus H(\mathrm{SID}_j \| N_2)$,$R_i = H(E_i \| F_i) \oplus H(N_1 \oplus N_2 \oplus N_3)$,$V_i = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))$,$T_i = N_2 \oplus N_3 \oplus H(E_i \| F_i \| N_1)$,网关节点把 (Q_i, R_i, V_i, T_i) 作为相互认证的信息发给传感器节点。

Step4: GWN → S_j: Q_i, R_i, V_i, T_i

传感器节点收到网关节点发送的信息 (Q_i, R_i, V_i, T_i),计算 $N_1 \oplus N_3 = Q_i \oplus H(\mathrm{SID}_j \| N_2)$,$H(E_i \| F_i) = R_i \oplus H(N_1 \oplus N_2 \oplus N_3)$,$V_i^* = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))$,并验证 V_i^* 是否等于 V_i。

Step5: S_j checks $V_i^* ? = V_i$

如果验证上述式子不成立,传感器节点就拒绝这次访问。如果验证上述等式成立,传感器节点就可以确认网关节点的合法性,并且传感器节点把 V_i, T_i 传送给用户。用户收到之后计算 $N_2 \oplus N_3 = T_i \oplus H(E_i \| F_i \| N_1)$,$V_i' = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))$,并验证 V_i' 是否等于 V_i。如果验证不相等,智能卡就拒绝这次访问;如果验证相等,智能卡就可以确认网关节点和传感器节点的合法性。

Step6: SmartCard checks $V_i' ? = V_i$

最终,用户 U_i,传感器节点 S_j,网关节点 GWN 达成了一个共享密钥 $\mathrm{SK} = H(H(E_i \| F_i) \| (N_1 \oplus N_2 \oplus N_3))$。

4.4　口令改变阶段

用户 U_i 有能力在网关节点不参与的情况下改变口令。用户 U_i 把他的智能卡插进读卡器,并且输入原始的身份和口令 ID_i^*, P_i^*,智能卡计算 $n = B_i \oplus H(\mathrm{ID}_i^* \| P_i^*)$,$E_i = H(n \| P_i^*)$,$J_i^* = H(\mathrm{ID}_i^* \| E_i)$,并验证 $J_i^* ? = J_i$。如果等式成立,用户就可以提交一个新的口令 P_i^{new},智能卡计算 $E_i^{\mathrm{new}} = H(n \| P_i^{\mathrm{new}})$,$J_i^{\mathrm{new}} = H(\mathrm{ID}_i \| E_i^{\mathrm{new}})$,$B_i^{\mathrm{new}} = n \oplus H(\mathrm{ID}_i \| P_i^{\mathrm{new}})$,$D_i^{\mathrm{new}} = F_i \oplus E_i^{\mathrm{new}}$,并把 $J_i^{\mathrm{new}}, B_i^{\mathrm{new}}, D_i^{\mathrm{new}}$ 存储在智能卡中替换 J_i, B_i, D_i。

5　改进方案的安全性分析

在提出的方案中,即使智能卡中的信息被攻击者提取出,攻击者也不能利用这些信息成功攻击这个方案。下面是安全性分析的具体细节。

5.1　智能卡丢失攻击

在这种攻击中,攻击者需要伪造一个登陆请求 $(G_i, H_i, D_i, y_i, \mathrm{CID}_i)$ 来假冒合法用户,然而攻击者并不能计算 $G_i = H(A_i) \oplus N_1$,$H_i = H(F_i \| E_i \| N_1)$,$D_i = E_i \oplus F_i$,$\mathrm{CID}_i = E_i \oplus H(G_i \| N_1)$,因为攻击者并没有 A_i, E_i, F_i。

假设用户 U_i 的智能卡丢失,攻击者可以提取出智能卡中的信息 $(J_i, D_i, B_i, g, y_{\mathrm{GWN}}, H(\cdot))$,但是攻击者得不到 x,也不能得到用户的 ID_i, P_i, n,所以攻击者计算不出 $A_i = y_{\mathrm{GWN}}^n \mathrm{mod} p$,$E_i = H(n \| P_i)$,$F_i = D_i \oplus E_i$,也就不能利用得到的智能卡进行假冒攻击。所以,该方案可以抵抗智能卡丢失攻击。

5.2　数据库泄露攻击

在 Sheetal Kalra 的方案中,如果网关节点的数据库中存储的数据 J_i 和 $y_i \oplus x$ 泄露给攻击者 U_k,攻击者就可以从中得到 x,进而得到每个用户的 y_i,所以可以进行假冒攻击。而文中方案的网关节点数据库中并没有存储任何有关用户和传感器节点的信息,所以攻击者不能利用数据库泄露得到用户的相关信息,也就不可能进行假冒攻击。

5.3　重放攻击

假设攻击者截获到用户和网关节点之间的信息,

想要把截获到的信息再次发送给网关节点来假冒合法用户。用户计算 $G_i = H(A_i) \oplus N_1$, $CID_i = E_i \oplus H(G_i \| N_1)$, $H_i = H(F_i \| E_i \| N_1)$, 网关节点计算 $Q_i = N_1 \oplus N_3 \oplus H(SID_j \| N_2)$, $R_i = H(E_i \| F_i) \oplus H(N_1 \oplus N_2 \oplus N_3)$, $V_i = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))$, $T_i = N_2 \oplus N_3 \oplus H(E_i \| F_i \| N_1)$, $M_i = H(SID_j \| x) \oplus N_2$, $K_i = H(H(SID_j \| x) \| N_2)$, 传感器节点计算 $M_i = H(SID_j \| x) \oplus N_2$, $K_i = H(H(SID_j \| x) \| N_2)$ 时, 每次通信都选取不同的 N_1, N_2, N_3 以保证每次发送的消息都是不同的, 所以重放攻击是无效的。

5.4 用户的匿名性

在注册阶段, 用户和网关节点之间是在安全信道中进行通信, 可以保护用户的身份。在登录阶段, 用户用 $CID_i = E_i \oplus H(G_i \| N_1)$ 代替真正的身份来登录, 所以攻击者不能得到真正的 ID_i。在认证和密钥共识阶段, 所有的计算都是在 E_i, F_i 的基础上进行的而不是真正的身份 ID_i。此外用户每次登录的动态身份 CID_i 包含随机数 N_1, 所以用户每次登陆的身份不同, 因此攻击者不能根据登录请求来判断具体是哪一个用户。

5.5 正确的相互认证和密钥共识

Sheetal Kalra 的方案不能达成正确的共享密钥, 因为传感器节点和网关节点不能得到用户的真正身份 ID_i, 但是在达成的共享密钥中却使用了用户 U_i 的真正身份 ID_i。Sheetal Kalra 方案的认证和密钥共识阶段中, 网关节点通过计算 $K_i^* = H(H(x) \| y_i \| SID_S \| N_1)? = K_i$ 验证传感器节点, 计算 $J_i^* = CID_i \oplus N_1 \oplus H(x) \oplus x? = J_i$ 来验证用户, 而在文中方案, 是通过计算 $K_i^* = H(H(SID_j \| x) \| N_2)? = K_i$ 来验证传感器节点, 通过计算 $H_i^* = H(E_i \| F_i \| N_1)? = H_i$ 来验证用户。相互认证时, 传感器节点通过计算 $V_i^* = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))? = V_i$ 来验证服务器, 用户通过计算 $V_i = H(H(E_i \| F_i) \| H(N_1 \oplus N_2 \oplus N_3))? = V_i$ 验证服务器。最终用户 U_i、传感器节点 S_j、网关节点 GWN 达成共享密钥 $SK = H(H(E_i \| F_i) \| (N_1 \oplus N_2 \oplus N_3))$, 因此, 文中方案可以提供正确的相互认证和共享密钥。

6 结束语

文中指出了 Sheetal Kalra 的方案容易在数据库泄露和用户智能卡丢失的情况下受到用户的假冒攻击, 而且, Sheetal Kalra 方案也不能提供正确的共享密钥。于是, 提出了一种新的相互认证和密钥共识方案。该方案可以满足无线传感器网络相互认证和密钥共识方案的所有安全需求。与 Sheetal Kalra 的方案以及其他相关方案相比, 该方案的网关节点数据库中并没有存储任何信息, 即使智能卡丢失, 攻击者也无法进行假冒攻击。此外, 该方案保证了用户在通信过程中的匿名性, 并提供了安全的共享密钥, 计算量也相对较小, 所以更安全、更高效。

参考文献:

[1] WATRO R, KONG D, CUTI S F, et al. TinyPK: securing sensor networks with public key technology[C]//Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks. [s. l.]: ACM, 2004: 59-64.

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

[3] HE D, GAO Y, 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.

[4] 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.

[5] CHEN T H, SHIH W. A robust mutual authentication protocol for wireless sensor networks[J]. ETRI Journal, 2010, 32(5): 704-712.

[6] HSIU-LIEN Y, CHEN T H, LIU P C, et al. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. Sensors, 2011, 11(5): 4767-4779.

[7] HE D, CHEN C, MA M, et al. A secure and efficient password-authenticated group key exchange protocol for mobile ad hoc networks[J]. International Journal of Communication Systems, 2013, 26(4): 495-504.

[8] HE D, KUMAR N, CHILAMKURTI N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks[C]//International symposium on wireless and pervasive computing. [s. l.]: [s. n.], 2015: 263-277.

[9] XUE K, MA C, HONG P, et al. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks[J]. Journal of Network & Computer Applications, 2013, 36(1): 316-323.

[10] KALRA S, SOOD S K. Advanced password based authentication scheme for wireless sensor networks[J]. Journal of Information Security & Applications, 2015, 20: 37-46.

[11] 赵泽茂. 数字签名理论[M]. 北京: 科学出版社, 2007.

[12] 张亦辰, 李继国, 汤 铭. 自认证公钥代理签名方案[J]. 北京电子科技学院报, 2005, 13(2): 19-22.

[13] 张兴华. 指定验证人无第三方代理多重签名方案[J]. 信息安全与通信保密, 2014(2): 85-87.

[14] 张玉磊, 周冬瑞, 李臣意, 等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2015, 36(2): 48-55.