



基于智能卡和密码保护的 WSN 远程用户安全认证方案

刘丽萍

(贵州交通职业技术学院信息工程系 贵阳 550008)

摘要:针对无线传感器网络(WSN)用户远程安全认证问题,分析现有方案的不足,提出一种新颖的基于智能卡的 WSN 远程用户认证方案。通过用户、网关节点和传感器节点之间的相互认证来验证用户和节点的合法性,并结合动态身份标识来抵抗假冒攻击、智能卡被盗攻击、服务拒绝攻击、字典攻击和重放攻击。同时对用户信息进行匿名保护,且用户能够任意修改密码。性能比较结果表明,该方案具有较高的安全性能,且具有较小的计算开销。

关键词:无线传感器网络;安全认证;智能卡;相互认证;密码保护

doi: 10.11959/j.issn.1000-0801.2015294

A Remote User Security Authentication Scheme Using Smart Card and Password Protection for WSN

Liu Liping

(Department of Information Technology, Guizhou Polytechnic College of Communications, Guiyang 550008, China)

Abstract: For the issues that the user remote security authentication for wireless sensor network (WSN), and the defects of the existing schemes, a remote user security authentication scheme of using smart card for WSN was proposed. The mutual authentication between the user, the gateway nodes and sensor nodes was used to verify the legitimacy of users and nodes. This scheme combines mutual authentication and dynamic identity to resist the impersonation attack, smart card stolen attack, distributed denial of service attack, dictionary attack and replay attack. At the same time, the user information was provided anonymous protection, and the user could change the password. The performance comparison results show that the proposed scheme has high security performance and small computational cost.

Key words: wireless sensor network, security authentication, smart card, mutual authentication, password protection

收稿日期:2015-07-23;修回日期:2015-10-29

基金项目:贵州省交通厅科技项目(No.2014321050)

Foundation Item: The Science and Technology Project of Guizhou Provincial Communications Department (No.2014321050)

论文引用格式:刘丽萍. 基于智能卡和密码保护的 WSN 远程用户安全认证方案. 电信科学, 2015294

Liu L P. A remote user security authentication scheme using smart card and password protection for WSN. Telecommunications Science, 2015294



1 引言

无线传感器网络(wireless sensor network, WSN)是一种由传感器节点组成,通过无线通信相连接的自组织网络。由于通信网络的发展,无线传感器已成为很多复杂网络的关键组件。但 WSN 通常工作在恶劣环境中,使其通信遭受到各种安全性威胁^[1]。目前,在传感器网络安全性研究方面,大多是关于网络内部节点之间传输的安全性,而对外部用户访问的安全问题考虑较少,然而,外部用户非法访问 WSN 内部节点获取数据会对网络安全造成严重影响^[2]。因此,如何验证外部用户和传感器节点身份的合法性尤为重要。

目前,已经提出了多种用于认证 WSN 合法用户的远程用户认证方案。参考文献[3]提出了一种基于散列函数对称加密的动态用户认证方案,然而其易受重放、伪造或口令被攻击。为此,参考文献[4]提出一种包含网关节点(GWN)的无线网络的双重认证方案,该方案基于散列函数和异或运算进行密码认证,计算效率较高,然而其并没有提供相互认证和会话密钥协商机制。参考文献[5]提出了一种认证方案,提供用户、GWN 和传感器节点之间的相互认证,但方案容易受到伪造和重放攻击。最近,研究者提出了几种基于椭圆曲线加密(elliptic curve cryptography, ECC)的认证方案。参考文献[6]提出了一种基于 ECC 的远程用户认证方案,相比其他方案,其计算成本较高。参考文献[7]提出一种分簇 WSN 节点身份认证机制,采用单向散列函数对密码和身份(ID)进行散列化,利用密码参与 ECC 签名算法的生成。然而,其源匿名信息的认证是通过一个方程而不是独立的验证签名。最近,参考文献[8]提出了一种用于 WSN 的基于时间证书的相互认证和密钥协商方案,该方案提供了用户、传感器节点和 GWN 之间的相互认证。但该方案容易受到假冒攻击、服务器欺骗攻击和被盗窃智能卡攻击。

本文针对参考文献[8]方案的缺陷,提出一种使用智能卡的 WSN 远程用户认证方案,可以提供用户、传感器和 GWN 三方之间的相互认证,使用随机值实现动态身份标识来抵抗重放攻击,同时能够抵抗字典攻击、智能卡被盗攻击等多种攻击。

2 参考文献[8]的认证方案

典型 WSN 通常包含 3 个通信实体:网络用户、传感器节点和网关^[9],WSN 基本通信架构如图 1 所示。传感器节

点、网关节点和用户设备彼此通信,需要一种安全、有效的认证方案进行相互认证,实现安全通信。

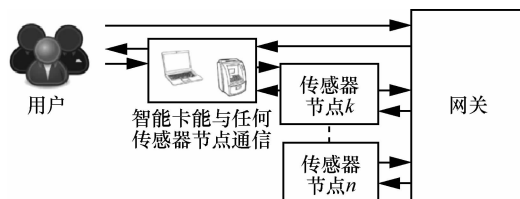


图 1 无线传感器网络的基本通信架构

参考文献[8]提出的基于智能卡的 WSN 远程用户认证方案包括 3 个阶段:注册阶段;登录阶段;认证和密钥协商阶段。详细的方案参见原文献。

通过对参考文献[8]的方案进行分析,发现其不能抵御假冒攻击、智能卡被盗攻击和服务器欺骗攻击,且用户无法修改密码。

(1) 假冒攻击

恶意授权用户可以利用自己的智能卡来收集信息 $\{H(\cdot), ID_i, H(H(PW_i)), TE_i, TC_i\}$ 获得 ID_i , 同时对 $H(H(PW_i))$ 运用暴力破解攻击^[10], 从而获得密码 PW_i 。使用这两个参数, 恶意用户可以生成有效的登录请求, 因此, 恶意用户可以很容易地得到验证, 并冒充合法用户。

(2) 智能卡被盗攻击

攻击者可以窃取合法用户的智能卡, 通过使用逆向工程技术, 提取智能卡中所存储的参数 $\{H(\cdot), ID_i, H(H(PW_i)), TE_i, TC_i\}$ 。通过暴力破解, 就可以从 $H(H(PW_i))$ 得到密码, 此时, 攻击者可以利用 ID_i 和 PW_i 产生有效的登录请求。因此, 该方案会受到智能卡被盗攻击。

(3) 服务器欺骗攻击

在该方案的开始阶段, 假定每个用户和传感器节点具有预先配置的标识和安全密码, 散列值存储在 GWN 端。攻击者可以随时欺骗 GWN 来收集用户 U_i 的身份标识 ID_i 、用户和传感器节点密码。之后, 攻击者可能会生成一个有效的登录请求, 并访问传感器节点的资源。因此, 该方案会受到服务器欺骗攻击。

(4) 离线字典攻击

正如上文所述, 方案假定用户和传感器共享身份标识, 并与 GWN 共享密码的散列值。随着技术的进步, 攻击者通过离线字典攻击可以很容易收集到这些信息。

(5) 无密码更新过程

用户 U_i 不能自由更新密码。相反, 静态密码由用户 U_i 与 GWN 共享, 可以被攻击者伪造。

(6) 时间戳的使用

方案中, 利用时间戳实现用户的动态身份认证, 然而其存在时间同步问题, 即用户和服务器的时钟难以同步。

3 本文提出的方案

本文提出一种无线传感器网络动态身份认证方案, 提供用户、GWN 和传感器节点之间的相互认证。在 GWN 注册成功后, 为合法用户分发智能卡, 合法用户插入智能卡后提交正确的证书可以容易地登录到 WSN 中, 方案中使用的符号列于表 1 中。本文方案包括 5 个阶段, 即注册、登录、认证、会话密钥协商和密码修改阶段。

表 1 本文方案用到的符号及含义

符号	含义
U_i	第 i 个用户
GWN	网关节点
S_s	第 s 个传感器节点
SID_s	传感器节点 S_s 的身份标识
SK_s	传感器节点 S_s 的唯一密钥
SK	通用会话密钥
ID_i	用户 U_i 的唯一身份标识
P_i	用户 U_i 密码
$H(\cdot)$	单向散列函数
y_i	用户 U_i 通过 GWN 选择随机值
X	GWN 的主密钥参数
N_1	由智能卡生成的随机值
N_2	由传感器节点生成的随机值
N_3	由 GWN 产生的随机值
$\oplus$	异或运算
	串联

(1) 注册阶段: 用户 U_i 通过安全通道提交身份 ID_i 和密码验证信息给 GWN。GWN 计算必要的安全参数, 并将它们存储在智能卡上, 颁发智能卡给用户。用户也计算并存储智能卡上的一些安全参数。

(2) 登录阶段: 用户 U_i 将智能卡插入读卡器并提交自己的身份标识 ID_i 和密码 P_i 。智能卡验证用户 U_i 的身份, 并发送验证信息到目标传感器节点。

(3) 认证阶段: 传感器节点转发用户和传感器验证信息给 GWN。验证用户后, 传感器节点和 GWN 发送一些安全参数给用户的智能卡。用户根据这些参数验证 GWN 和传感器节点的真实性。

(4) 会话密钥协商阶段: 一旦完成相互认证, GWN、传

感器节点和用户商定共同会话密钥, 保证下一步通信安全。

(5) 密码修改阶段: 用户 U_i 能够改变自己的密码, 无需 GWN 干预。

3.1 注册阶段

用户 U_i 选择一个随机数 n , 计算安全参数 $E_i = H(ID_i | n)$ 、 $F_i = H(n \oplus P_i)$, 并通过安全信道提交 E_i 和 F_i 给 GWN。

步骤 1 $U_i \rightarrow GWN: E_i, F_i$

GWN 计算安全参数 $G_i = E_i \oplus y_i$ 、 $H_i = F_i \oplus H(y_i) \oplus H(x)$ 和 $J_i = E_i \oplus H(y_i) \oplus x$, 其中 x 是 GWN 的密钥, y_i 是 GWN 为用户 U_i 选择的随机数, 使 J_i 值对于每个用户唯一。GWN 在自己的客户端数据库存储对应 J_i 的 $y_i \oplus x$ 。最后, GWN 通过安全信道发出包含安全参数 $(G_i, H_i, H(\cdot))$ 的智能卡给用户。

步骤 2 $GWN \rightarrow U_i$: 智能卡

一旦用户获取到智能卡, 则计算安全参数 $A_i = n \oplus H(ID_i | P_i)$ 、 $B_i = H(ID_i | P_i) \oplus P_i$, 并在智能卡中输入 A_i 和 B_i 的值, 智能卡中将安全参数 $(A_i, B_i, G_i, H_i, H(\cdot))$ 保存在其内存中。

无线网络中的每个传感器节点也将 GWN 上进行注册, 每个传感器节点和 GWN 商定一个唯一的密钥 SK_s , GWN 存储密钥 SK_s 为 $SK_s \oplus H(x | SID_s)$, 对应于服务提供者数据库中的服务器身份标识 SID_s 。

3.2 登录阶段

用户 U_i 将智能卡插入读卡器, 输入 ID_i^* 和密码 P_i^* 。智能卡计算 $B_i^* = H(ID_i^* | P_i^*) \oplus P_i^*$, 并与存储器中存储的 B_i 值进行比较, 以验证用户 U_i 的合法性。

步骤 1 智能卡验证 $B_i^* = B_i$

验证后, 智能卡生成随机值 N_1 并计算 $n = A_i \oplus H(ID_i | P_i)$ 、 $E_i = H(ID_i | n)$ 、 $F_i = H(n \oplus P_i)$ 、 $y_i = G_i \oplus E_i$ 、 $H(x) = H_i \oplus F_i \oplus H(y_i)$ 、 $C_i = H^2(x) \oplus N_1$ 、 $CID_i = E_i \oplus H(y_i) \oplus H(x) \oplus N_1$ 和 $K_i = H(H(x) | y_i | N_1)$, 这些请求信息在每次登录时动态变化。然后智能卡发送登录请求信息 $(C_i | CID_i | K_i)$ 给 GWN。

步骤 2 智能卡 $\rightarrow GWN: (C_i | CID_i | K_i)$

网关节点将请求传递到距离最近、可用且 ID 为 SID_s 的传感器节点。

3.3 认证阶段

ID 为 SID_s 的传感器节点接收来自用户 U_i 发送的登录请求后, 生成随机数 N_2 , 计算 $D_i = N_2 \oplus SK_s$, 并发送登录请求信息 $(SID_s, C_i, CID_i, K_i, D_i)$ 给 GWN。

步骤 1 $S_j \rightarrow GWN: SID_s, C_i, CID_i, K_i, D_i$

GWN 从 $SK_s \oplus H(x | SID_s)$ 提取 SK_s , 对应于其数据库中无线传感器节点的 SID_s 。GWN 计算 $N_1 = C_i \oplus H^2(x)$ 、 $N_2 = D_i \oplus SK_s$ 、



$J_i^* = CID_i \oplus N_1 \oplus H(x) \oplus x$, 从其与无线网络用户相关的数据库寻找对应于 J_i^* 的 J_i 的匹配值。

步骤 2 GWN 认证 $J_i^*? = J_i$

如果 J_i^* 值不与用户数据库中任意 J_i 值匹配, 则拒绝登录请求, GWN 终止会话; 否则, GWN 从用户数据库中对应于 J_i^* 的 $y_i \oplus x$ 中提取 y_i 。GWN 计算 $K_i^* = H(H(x)|y_i|SID_i|N_1)$ 后, 比较 K_i^* 与接收到的 K_i 值来验证用户和传感器节点 S_i 的合法性。

步骤 3 GWN 认证 $K_i^*? = K_i$

若 K_i^* 与 K_i 值不匹配, 则 GWN 拒绝登录请求并终止通信会话。否则, GWN 生成随机值 N_3 , 并计算 $M_i = N_1 \oplus N_3 H(SK_i | N_2)$ 、 $R_i = H(CID_i | y_i | N_1) \oplus H(N_1 \oplus N_2 \oplus N_3)$ 、 $V_i = H[H(N_1 \oplus N_2 \oplus N_3) | H(CID_i | y_i | N_1)]$ 、 $W_i = N_2 \oplus N_3 \oplus H(y_i | CID_i | H(x) | N_1)$, 回传安全参数给传感器节点 S_i 。传感器节点使用 M_i 计算 $N_1 \oplus N_3$, 使用 R_i 计算 $H(CID_i | y_i | N_1)$, 然后计算 $V_i^* = H[H(N_1 \oplus N_2 \oplus N_3) | H(CID_i | y_i | N_1)]$ 。比较 V_i^* 的计算值与 V_i 的接收值来验证网关节点 GWN 的合法性。

步骤 4 传感器节点验证 $V_i^*? = V_i$

传感器节点 S_i 发送 (V_i, W_i) 给用户 U_i 的智能卡, 智能卡计算 $N_2 \oplus N_3 = W_i \oplus H(y_i | CID_i | H(x) | N_1)$ 、 $V_i^* = H[H(N_1 \oplus N_2 \oplus N_3) | H(CID_i | y_i | N_1)]$, 并比较接收到的 V_i 值和 V_i^* 的计算值。GWN 和传感器节点 S_i 之间的这种相互认证用来确认每个实体的合法性。

3.4 会话密钥协商阶段

上述相互认证成功后, 用户 U_i 的智能卡、传感器节点 S_i 和网关节点 GWN 商定共同的会话密钥 $SK = H(H(ID_i | P_i) | (N_1 \oplus N_2 \oplus N_3))$ 。所有用户 U_i 、传感器节点 S_i 和网关节点 GWN 之间的通信信息用会话密钥异或运算, 保证了 3 个实体之间通信的安全性。

3.5 密码修改阶段

用户 U_i 能够修改自己的密码, 无需 GWN 的干预。用户将自己的智能卡插入读卡器并输入自己的身份 ID_i^* 和密码 P_i^* 。智能卡计算安全参数 $B_i^* = H(ID_i^* | P_i^*) \oplus P_i^*$, 并比较 B_i^* 的计算值与其内存中 B_i 的存储值来验证用户 U_i 的合法性。智能卡持有人认证后, 智能卡计算值 $b = H(y_i)$ 、 $H(x)$, 系统会提示用户重新提交新密码 P_i^{new} 。用 $A_i^{new} = b \oplus H(ID_i | P_i^{new})$ 、 $B_i^{new} = H(ID_i | P_i^{new}) \oplus P_i^{new}$ 和 $H_i = H(b \oplus P_i^{new}) \oplus H(y_i) \oplus H(x)$ 更新存储在持有者智能卡中的安全参数值 $A_i = b \oplus H(ID_i | P_i)$ 、 $B_i = H(ID_i | P_i) \oplus P_i$ 和 $H_i = H(b \oplus P_i) \oplus H(y_i) \oplus H(x)$ 。以此提供一个有效的密码更改阶段。

4 安全性分析

很多基于智能卡的方案容易受到各种安全攻击, 通过使用各种逆向工程技术可以提取存储在智能卡上的信息^[11]。本文提出的方案中, 即使恶意用户能够提取智能卡中的信息, 也不能成功登录网络。

(1) 假冒攻击

假冒攻击中, 攻击者伪造从通信信息收集的认证信息, 并冒充为合法用户。攻击者必须猜测 E_i 、 $H(x)$ 、 y_i 来伪装成合法用户 U_i 登录到无线传感器网络。在提出的方案中, 不可能在实时多项式时间内正确猜出所有安全参数。并且, 攻击者也不能在安全通道上通过截获通信参数 C_i 、 CID_i 、 K_i 、 D_i 、 M_i 、 R_i 、 V_i 、 W_i 来计算 E_i 、 $H(x)$ 、 y_i 。因此, 本文方案能抵抗假冒攻击。

(2) 被盗智能卡攻击

合法用户 U_i 的智能卡可能被恶意用户盗取, 并提取出存储在智能卡上的安全信息: $A_i = n \oplus H(ID_i | P_i)$ 、 $B_i = H(ID_i | P_i) \oplus P_i$ 、 $G_i = E_i \oplus y_i$ 和 $H_i = F_i \oplus H(y_i) \oplus H(x)$ 。获取这些信息后, 恶意用户必须在多项式时间内同时猜测至少两个安全参数, 然而这是做不到的。因此, 本文方案能够抵抗智能卡被盗窃攻击。

(3) 服务拒绝攻击

攻击者获得合法用户的智能卡, 并修改存储在智能卡上的验证信息, 使用户 U_i 不能够登录到无线网络, 无法获取正常服务^[12]。本文方案中, 在用户 U_i 密码更新过程之前, 智能卡会检查身份标识 ID_i 和密码 P_i 的有效性。恶意用户得到合法用户的智能卡, 将智能卡插入读卡器设备, 并尝试猜测用户 U_i 的身份 ID_i 和密码 P_i 。由于智能卡计算 $B_i^* = H(ID_i^* | P_i^*) \oplus P_i^*$, 并用 B_i 的存储值进行比较, 在接受密码更新请求之前验证用户 U_i 的真实性。同样由于不可能在多项式时间内同时猜测身份 ID_i 和密码 P_i , 所以本文方案能够抵抗服务拒绝攻击。

(4) 字典攻击

在线字典攻击中, 恶意用户试图字典猜测各种密码, 以获得对无线网络的访问。离线字典攻击中, 恶意用户记录通信消息, 并尝试从记录的消息中离线猜测用户身份 ID_i 和密码 P_i ^[13]。本文方案中, 即便获得合法用户的有效智能卡, 恶意用户也必须同时猜测对应于用户 U_i 的身份 ID_i 和密码。用户最多有 3 次机会来注册网络, 之后智能卡会被锁定。因此, 本文方案能够抵抗字典攻击。

(5)重放攻击

恶意用户首先监听用户 U_i 和 GWN 之间的通信信息, 然后通过重发捕捉消息, 试图模仿合法用户^[14]。本文方案中, 这种尝试肯定会失败, 因为用户智能卡、GWN 和传感器节点在每个新会话会选择不同的随机值 (N_1, N_2, N_3) 。所有身份信息均为动态变化, 重传这些信息是无用的。此外, 攻击者不能够计算会话密钥 $SK=H(H(ID_i|y_i|N_1)|(N_1\oplus N_2\oplus N_3))$, 因为智能卡、GWN 和传感器节点在每一个新的会话中会选择不同的随机值 $(N_1\oplus N_2\oplus N_3)$, 且恶意用户不知道 ID_i 、 y_i 、 N_1 、 N_2 、 N_3 值。因此, 本文方案能够抵抗重放攻击。

(6)相互认证

本文方案实现了智能卡、GWN 和传感器节点三大通信实体的相互认证。三方分别给出自己的随机值 N_1 、 N_2 、 N_3 来共同推导会话密钥 $SK=H(H(ID_i|y_i|N_1)|(N_1\oplus N_2\oplus N_3))$ 。GWN 使用验证信息 $K_i^*=H(H(x)|y_i|SID_i|N_1)$ 认证用户 U_i , 传感器节点使用 $V_i^*=H[H(N_1\oplus N_2\oplus N_3)|H(CID_i|y_i|N_1)]$ 认证 GWN, 用户 U_i 使用 $V_i^*=H[H(N_1\oplus N_2\oplus N_3)|H(CID_i|y_i|N_1)]$ 认证传感器节点。

(7)身份匿名保护

本文方案对用户提供了身份匿名保护, 在认证过程中不是验证用户 U_i 的真实身份 ID_i , 而是产生一个伪标识 $CID_i=E_i\oplus H(y_i)\oplus H(x)\oplus N_1$, 且动态变化, 用于合法用户 U_i 到传感器节点和 GWN 的认证。用户的真实身份信息从不在登录、认证和会话密钥协商阶段进行传输。

5 性能比较

将本文方案与现有 WSN 用户认证方案进行安全性能比较, 结果见表 2, 其中, Y 表示达到该功能或能够抵抗该攻击, N 表示未达到或不能抵抗。

有效认证方案必须考虑通信和计算成本, 假设身份标

识 ID_i 、密码 P_i 、 x 、 y_i 随机值 (N_1, N_2, N_3) 都是 64 bit。比较中考虑 2 种计算量较高的主要运算^[15]; T_H 表示一次散列运算所需时间, T_{ECC} 表示一次 ECC 加密/解密操作所需时间。令 $E1$ 、 $E2$ 、 $E3$ 分别为用户、GWN 和传感器节点的计算开销。不同方案的计算开销 $E1$ 、 $E2$ 、 $E3$ 比较结果见表 3。

表 3 各种方案的计算开销比较

方案	E_1	E_2	E_3
本文方案	$10T_H$	$7T_H$	$7T_H$
参考文献[8]方案	$8T_H$	$11T_H$	$6T_H$
参考文献[6]方案	$4T_H+3T_{ECC}$	$6T_H+5T_{ECC}$	$4T_H+3T_{ECC}$
参考文献[7]方案	$2T_H+2T_{ECC}$	$5T_H+4T_{ECC}$	$2T_H+3T_{ECC}$
参考文献[4]方案	$5T_H$	$7T_H$	$4T_H$
参考文献[5]方案	$7T_H$	$8T_H$	$4T_H$

从表 2 可以看出, 本文方案增强了安全性能和对攻击的抵抗能力, 能够更好地保障智能卡用户免受恶意服务器的潜在危害。从表 3 可以看出, 相比于其他方案, 本文方案在保证较高安全性能的前提下, 其计算复杂度略小, 更适合 WSN 用户安全认证的应用场景。

6 结束语

本文分析了参考文献[8]方案存在效率不高且易遭受安全性攻击, 提出一种新颖的基于智能卡的 WSN 远程用户认证方案, 通过用户、传感器节点和 GWN 之间的相互认证来验证合法用户, 同时用户能够任意修改密码, 并对用户信息提供匿名保护。本文方案还能够抵抗假冒攻击、智能卡被盗攻击、服务拒绝攻击、字典攻击和重放攻击。在保证高安全性能的同时, 具有较小的计算开销。

未来工作中, 将考虑使用密码学中的随机预言模型来测试本文方案的安全性能。

表 2 各种方案之间的功能对比

方案	本文方案	参考文献[8]方案	参考文献[6]方案	参考文献[7]方案	参考文献[4]方案	参考文献[5]方案
密钥协商	Y	Y	Y	Y	N	Y
相互认证	Y	Y	Y	Y	N	Y
密码更新	Y	N	N	N	N	Y
身份匿名保护	Y	N	Y	Y	Y	Y
假冒攻击	Y	N	Y	Y	N	N
智能卡被盗攻击	Y	N	N	Y	N	N
服务拒绝攻击	Y	N	Y	Y	Y	Y
字典攻击	Y	N	Y	N	Y	Y
重放攻击	Y	N	N	Y	Y	N
伪装攻击	Y	N	Y	N	N	N



参考文献

- 1 管亚洲, 刘文芬, 魏江宏等. 适用于无线传感器网络的动态 ID 认证方案. 密码学报, 2014, 1(5):422~436
Zan Y Z, Liu W F, Wei J H, *et al.* A novel dynamic ID-based user authentication scheme for wireless sensor networks using smart cards. Journal of Cryptologic Research, 2014, 1(5): 422~436
- 2 王小刚, 石为人, 周伟等. 一种基于二次型的无线传感器网络密钥管理方案. 电子学报, 2013, 41(2):214~219
Wang X G, Shi W R, Zhou W, *et al.* A key management scheme based on quadratic form for wireless sensor network. Acta Electronica Sinica, 2013, 41(2):214~219
- 3 Vaidya B, Makrakis D, Mouftah H T. Improved two-factor user authentication in wireless sensor networks. Proceedings of IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications(WiMob), Shenzhen, China, 2010: 600~606
- 4 Mnif A, Cheikhrouhou O, Jemaa M B. An ID-based user authentication scheme for wireless sensor networks using ECC. Proceedings of 2011 International Conference on Microelectronics (ICM), Nanjing, China, 2011:1~9
- 5 Huang X, Dharmendra S, Cui H Y. Fuzzy controlling window for elliptic curve cryptography in wireless sensor networks. Proceedings of the International Conference on Information Networking 2014 (ICOIN2014), Xiamen, China, 2014: 312~317
- 6 Faye Y, Guyennet H, Niang I, *et al.* Fast scalar multiplication on elliptic curve cryptography in selected intervals suitable for wireless sensor networks. Lecture Notes in Computer Science, 2013(1):171~182
- 7 周治平, 庄学波. 基于 P-ECC 和同余方程的分簇 WSN 节点身份认证机制. 计算机应用, 2014, 34(1):104~107
Zhou Z P, Zhuang X B. Node identity authentication scheme for clustered WSNs based on P-ECC and congruence equation. Journal of Computer Applications, 2014, 34(1):104~107
- 8 Xue K, Ma C, Hong P, *et al.* A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network & Computer Applications, 2013, 36(1):316~323
- 9 刘云, 杨亮, 范科峰等. 一种改进的动态用户认证协议. 电子学报, 2013, 41(1):42~46
Liu Y, Yang L, Fan K F, *et al.* Improved dynamic user authentication protocol. Acta Electronica Sinica, 2013, 41(1):42~46
- 10 戚湧, 高双双, 李千目. 基于动态软键盘和随机码的 Web 口令安全传输. 南京理工大学学报, 2014, 38(6):745~749
Qi Y, Gao S S, Li Q M. Security transfer of Web password based on dynamic soft keyboard and random code. Journal of Nanjing University of Science and Technology, 2014, 38(6):745~749
- 11 Pippal R S, Gupta P, Singh R. A novel smart card authentication scheme using image encryption. International Journal of Computer Applications, 2013, 72(9):8~14
- 12 Wei J H, Liu W F, Hu X X. Cryptanalysis and improvement of a robust smart card authentication scheme for multi-server architecture. Wireless Personal Communications, 2014, 77 (3): 2255~2269
- 13 Li X, Niu J W, Kumari S, *et al.* An enhancement of a smart card authentication scheme for multi-server architecture. Wireless Personal Communications, 2015, 80(1):175~192
- 14 汪定, 马春光, 翁臣等. 一种适于受限资源环境的远程用户认证方案的分析与改进. 电子与信息学报, 2012, 34(10): 2520~2526
Wang D, Ma C G, Weng C, *et al.* Cryptanalysis and improvement of a remote user authentication scheme for resource-limited environment. Journal of Electronics & Information Technology, 2012, 34(10):2520~2526
- 15 张青. 基于智能卡的多服务器环境下的远端认证协议. 计算机应用研究, 2014, 31(7):2109~2115
Zhang Q. Remote authentication protocol for multi-servers based on smart card. Application Research of Computers, 2014, 31(7): 2109~2115

[作者简介]



刘丽萍, 女, 贵州交通职业技术学院讲师, 主要研究方向为信息安全、网络安全。