

基于无线传感器网络的双因子认证协议的设计与研究

齐爱琴¹, 申永军²

(1 西北民族大学 数学与计算机科学学院, 甘肃 兰州 730000;

2 兰州大学 信息科学与工程学院, 甘肃 兰州 730000)

摘 要: 认证技术是当今网络安全发展的一个重要方向. 无线传感器网络由于结点的资源和计算能力的限制, 简单有效的认证协议是其需要考虑的重要问题. 然而研究发现 M. L. Das 和 Khan 的协议都有一些安全缺陷, 本文提出了一种适用于无线传感器网络的双因子认证协议, 并对协议进行了安全分析和性能测试. 结果表明, 该协议能应对多种攻击, 系统安全性高.

关键词: 双因子; 智能卡; 认证

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)01-0121-03

Design and Research of Double Factor Authentication Protocol Based on Wireless Sensor Networks

QI Ai-qin¹, SHEN Yong-jun²

(1 School of Mathematics and Computer Science, Northwest University for Nationalities, Lanzhou 73000, China;

2 School of Information Science & Engineering, Lanzhou University, Lanzhou 73000, China)

Abstract: Because of the limitation of the resource and computing capability for wireless sensor networks a simple and efficient authentication protocol need to be taken into account. It was found that M. L. Das and Khan's protocols have a few security flaws. Therefore, This paper presents a double factor authentication protocol applying to wireless sensor networks and makes the security analysis and performance testing. The results show that the protocol has high security, which can cope with the multiple attacks.

Key words: double factor; smart card; authentication

1 引言

无线传感器网络由于易于实现、使用范围广等特点, 获得了市场的广泛应用. 然而安全问题也日益突出^[1], 许多专家和学者采用了多种技术来增强无线传感器网络的安全^[2-3].

认证作为安全应用系统的第一道防线, 是重要的安全服务. 由于传感器结点资源和计算能力的限制^[4], 一种简单有效的认证协议是无线传感器网络需要考虑的重要问题. 在 2009 年, M. L. Das 提出了双因子的认证协议^[5], 一个用户必须提供密码和智能卡两项内容来证明他的身份, 在实现中使用哈希

函数和异或运算, 这种特点适合于资源受限的环境. 然而, Khan 与 Algahather 的论文^[6]中指出 Das 的结构有一些缺点, 并且对于多种攻击是脆弱的. 研究发现, Khan 和 Das 的结构都有安全缺点, 仍然有对各种攻击的脆弱性.

文中提出了一个适用于无线传感器网络的双因子认证协议, 来应对各种攻击. 对于提出协议进行了安全分析, 结果显示了对各种攻击的强健性, 相比于以前的协议, 它更强健, 安全性更高.

2 协议中使用的参数说明

认证协议中的相关参数说明如表 1 所示.

表 1 协议有关的参数说明

MD: 用户	sn : 传感器结点
GW: 网关结点	Id_i, Id_s : 用户身份标识, 智能卡的标识
pw_i : 用户的密码	K : 网关生成的密钥
x_s : 网关产生的秘密值也存储在 一些 sn 结点中	$h(\cdot)$: 哈希函数
$M_1 \parallel M_2$: M_1 与 M_2 的连结	$\oplus$: 异或运算
T_i : 当前时间戳; $i=1, 2, 3, 4, 5$	ΔT : 传输延迟的合适时间间隔

3 无线传感器网络的双因子认证协议

认证协议由注册阶段、登录阶段、认证阶段、密钥交换阶段四个部分组成。

3.1 注册阶段

用户 MD 选取随机数 b , 身份标识 Id_i 和密码 pw_i , 计算 $\gamma_i = h(pw_i \parallel b)$, 发送 (Id_i, γ_i) 给网关结点 GW, 网关结点计算

$$\eta_i = h(Id_i \parallel \gamma_i \parallel x_s) \oplus h(K)$$

$$\alpha_i = h(\gamma_i \oplus x_s)$$

$$\beta_i = x_s \oplus h(Id_i \parallel \gamma_i)$$

将 $(Id_i, Id_s, h(\cdot), \eta_i, \alpha_i, \beta_i)$ 注入智能卡中, 并通过安全通道发给用户, 用户对智能卡进行修改, 将随机数 b 输入智能卡中, 最终智能卡包含的内容有 $(Id_i, Id_s, h(\cdot), \eta_i, \alpha_i, \beta_i, b)$ 。

3.2 登录阶段

用户将智能卡插入终端, 输入 Id_i, pw_i 和 b , 进一步计算 $\gamma_i^* = h(pw_i \parallel b)$, $x_s = \beta_i \oplus h(Id_i \parallel \gamma_i^*)$, $\alpha_i^* = h(\gamma_i^* \oplus x_s)$, 验证 α_i^* 与 α_i 是否相等。若相等则计算 $DID_i = h(Id_i \parallel \gamma_i^* \parallel x_s) \oplus h(x_s \parallel T)$, $\epsilon_i = h(\eta_i \parallel x_s \parallel T)$, T 为当前的时间戳, 将 (DID_i, ϵ_i, T) 发给 GW。

3.3 认证阶段

网关验证是否 $(T_1 - T) \leq \Delta T$, 计算 $x^* = DID_i \oplus h(x_s \parallel T)$, $\epsilon_i^* = h((x^* \oplus h(K)) \parallel x_s \parallel T)$, 验证 ϵ_i^* 与 ϵ_i 是否相等, 若相等则计算 $\sigma_i = h(DID_i \parallel sn \parallel x_s \parallel T_1)$, 发送 (DID_i, σ_i, T_1) 给 sn 结点。 sn 结点验证是否 $(T_2 - T_1) \leq \Delta T$, 计算 $\sigma_i^* = h(DID_i \parallel sn \parallel x_s \parallel T_1)$, 验证 σ_i^* 与 σ_i 是否相等, 若相等则计算 $U_i = \sigma_i \oplus x_s$, $\omega_i = h(U_i \parallel x_s \parallel T_2)$, 发送 (ω_i, T_2) 给网关结点。网关结点验证是否 $(T_3 - T_2) \leq \Delta T$, 若符合则计算 $U_i^* = \sigma_i \oplus x_s$, $\omega_i^* = h(U_i^* \parallel x_s \parallel T_2)$, 验证 ω_i^* 与 ω_i 是否相等, 若相等发送接受消息给 sn 结点, sn

结点计算 $\rho = h(DID_i \parallel sn \parallel x_s \parallel T_4)$, 发送 (sn, T_4, ρ) 给移动用户 MD, 移动结点验证是否 $(T_5 - T_4) \leq \Delta T$, 若符合则计算 $x_s = \beta_i \oplus h(Id_i \parallel \gamma_i)$, $\rho^* = h(DID_i \parallel sn \parallel x_s \parallel T_4)$, 验证 ρ^* 与 ρ 是否相等, 若相等则认证过程结束。

3.4 密钥更新阶段

用户输入 Id_i, pw_i, b 和 pw_m , 计算 $\gamma_i^* = h(pw_i \parallel b)$, $x_s = \beta_i \oplus h(Id_i \parallel \gamma_i^*)$, $\alpha_i^* = h(\gamma_i^* \oplus x_s)$, 验证 α_i^* 与 α_i 是否相等。若相等则随机选取随机数 b' 计算 $\eta_m = \eta_i \oplus h(Id_i \parallel \gamma_i \parallel x_s) \oplus h(Id_i \parallel h(pw_m \parallel b') \parallel x_s)$, $\alpha_m = h(h(pw_m \parallel b') \oplus x_s)$, $\beta_m = x_s \oplus h(Id_s \parallel h(pw_m \parallel b'))$, 用 $\eta_m, \alpha_m, \beta_m, b'$ 代替 $\eta_i, \alpha_i, \beta_i, b$, 密钥更新阶段结束。

4 安全及性能分析

无线传感器网络的双因子认证协议能抵抗以下几种攻击:

(1) 抗被盗智能卡攻击: 假定智能卡被盗或丢失, 恶意分子可以从智能卡中提取出 $(\eta_i, \alpha_i, \beta_i, b)$, 运用这些参数, 恶意分子尽力假冒成用户完成到网关结点的登录。但是, 他必须产生一个有效的请求消息 (DID_i, ϵ_i, T) , 而恶意分子不可能从 γ_i, x_s 中计算出 DID_i, ϵ_i , 从而不能生成请求消息, 该协议实现抗被盗智能卡攻击。

(2) 抗假冒网关攻击: 假定恶意分子从传感器结点获知 (sn, x_s) , 恶意分子也窃听登录消息多次, 例如: T_1 时间的消息 $(DID_{i1}, \epsilon_{i1}, T_1)$ 和 T_2 时间的 $(DID_{i2}, \epsilon_{i2}, T_2)$ 。然而当 γ_i 随着 pw_i, b 变化而改变时, 他不能从以前的登录消息中获得 $h(Id_i \parallel \gamma_i \parallel x_s)$, 从而不能假冒网关。

(3) 抗伪造攻击: 假定恶意分子通过执行结点捕获攻击, 从传感器结点中获取 (sn, x_s) , 在登录/认证阶段, 在不知道 σ_i 的情况下不能计算 ω_i , 从而不能产生有效消息 (ω_i, T_2) , 故不能假冒传感器结点进行伪造攻击。

(4) 抗密码猜测攻击: 由于网关和智能卡不包含密码/验证表, 从而抵御离线密码猜测攻击。

(5) 抗绕过网关攻击: 由于 x_s 不存储在智能卡中, 在不知道 x_s 时无法计算 DID_i , 从而无法绕过网关。同时没有来自网关的最后接受消息, 传感器结点对用户的请求不响应, 因此恶意分子不能绕过网关。

(6) 抗内部攻击: 在注册阶段, 用户发送 γ_i 给网关, γ_i 是哈希密码, 从而有效阻止内部攻击。

(7) 双向认证: 网关和传感器结点, 移动节点与

传感器结点之间实现了双向认证。

表 2 显示了和前面提到协议的安全性比较结果。

表 2 安全性比较			
协议	Das 协议	Khan-Algathbar 协议	本文协议
安全属性			
抗密码猜测攻击	部分	有	有
抗绕过网关攻击	没有	有	有
抗内部攻击	没有	有	有
双向认证	没有	部分	有
抗假冒网关攻击	没有	有	有
安全的更新或者变换密码	没有	没有	有
抗智能卡被盗攻击	没有	没有	有

在性能分析时,文中采用计算负载作为评价协议性能的指标。表 3 显示了和前面提到的协议进行的性能比较,比较参数是哈希函数运算时间和执行异或运算时间。

表 3 计算负载比较		
协议	阶段	阶段
	注册阶段(包括 MD 结点和 GW 结点)	登录及认证阶段(包括 MD 结点、Sn 结点和 GW 结点)
Das 协议	3 次哈希运算 1 次异或运算	8 次哈希运算 3 次异或运算
Khan-Algathbar 协议	3 次哈希运算 1 次异或运算	11 次哈希运算 3 次异或运算
本文协议	5 次哈希运算 3 次异或运算	16 次哈希运算 7 次异或运算

从上面分析中可以看出,计算负载有少量增加,但安全性明显提高。同时随着结点计算能力的进一

步增加,这些计算量是在可接受的范围之内。

5 结束语

本文提出了一个适用于无线传感器网络的双因子认证协议,并对协议进行了安全和性能分析,结果显示协议是相对安全和强健的。随着无线传感器网络的广泛应用,需要进一步改进协议来应对新的攻击和挑战。

参考文献:

[1] Chong C Y, Kumar S. Sensor networks: evolution, opportunities and challenges[J]. proceedings of IEEE, 2003, 91(8):1247-1256.

[2] 曾夏玲, 梁艳招, 彭雅丽, 等. 基于簇的无线传感器网络入侵检测系统[J]. 微电子学与计算机, 2008, 25(6):156-158.

[3] 肖政宏, 谢赞福, 陈志刚. 无线传感器网络中一种基于流量预测和相关系数的异常检测方法[J]. 微电子学与计算机, 2009, 26(7):214-216.

[4] E H(Jr). Callaway, wireless sensor networks, architectures and protocols[M]. auerbach publications, 2003.

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

[6] 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.

作者简介:

齐爱琴 女, (1979—), 硕士, 讲师. 研究方向为网络信息安全.

申永军 男, (1957—), 博士, 副教授. 研究方向为网络信息安全.