一种改进的动态用户认证协议

刘 云[1],杨 亮[1],范科峰[2],王 勇[3],唐仕军[3]
(1.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2.中国电子技术标准化研究院,北京 100007; 3.桂林电子科技大学电子工程与自动化学院,广西桂林 541004)

摘 要: 介绍了无线传感器网络中典型的动态用户认证协议,并指出了其优点和问题.在引入一种新的无线传感器网关结构的基础上提出了对动态用户认证协议的改进方案.分析表明:改进的协议保留了原协议高效、低耗的特点并加强了安全性和增加了用户便利性.

关键词: 无线传感器网络; 动态认证协议; 网络安全
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2013)01-0042-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.01.008

Improved Dynamic User Authentication Protocol

LIU Yun[1], YANG Liang[1], FAN Ke-feng[2], WANG Yong[3], TANG Shi-jun[3]
(1. *Key Laboratory of CNIS, MOE, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *China Electronics Standardization Institute, Beijing* 100007, *China*;
3. *Electronic Engineering and Automation College, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*)

Abstract: We introduce the classic dynamic user authentication protocols in WSNs (wireless sensor network), and analyze its advantage and problem. We introduce a new WSNs gateway structure. Base on it, we propose an improved dynamic user authentication protocol. The analysis shows the improved protocol keeps the original characteristics of high efficiency and low consumption, and it enhances security and increases the user's convenience.

Key words: WSNs; dynamic user authentication protocol; network security

1 引言

传感器网络的安全问题,一般被归纳为两个方面:外部安全和内部安全[1].本文主要关注外部安全中的用户认证问题[2].

传感器网络的各类认证协议包括基于公钥算法的认证协议、基于秘密共享的认证协议、动态认证协议等.其中动态认证协议由于没有使用复杂的密码算法、整体认证速度比较快等特点在无线传感器网络中应用普遍.下面介绍各种动态认证协议的特点及优劣.

1.1 Wong 动态认证协议存在的问题

动态用户认证协议[3]是最早由 Wong 提出的一种轻量级的、基于强口令的无线传感器网络用户认证协议,这种协议基于 C C Lee 在文献[4]中提出的一种改进型低通信消耗的移动通信用户认证方案.这类协议在无线传感器网络内部设置登录节点,用户通过登录节点经由网关进行认证.该协议将低消耗的用户认证协议引入无线传感器网络,用很小的计算和通信开销达到对动态用户认证的效果,但是这一协议存在一些安全问题:无法抵抗重放和伪造攻击;口令可以被任意传感器网络节点获取;用户无法更换口令.

1.2 Tseng 改进动态认证协议存在的问题

Tseng、Lee-Chun Ko 等人提出一种针对上述认证协议的改进方法[5].Tseng 等人的方案[6],很好的解决原有协议的一些安全问题,保留了原协议低通信消耗、低运算量的特点.存在的问题主要是攻击者可以伪装网关重放攻击.攻击者可以在重放之前监听到的正确的用户申请,之后阻塞登录节点到网关的消息传输,然后重放网关监听到的以前的认证许可消息,重放给登录节点,登录节点将被欺骗,攻击者认证成功.

1.3 Lee-Chun Ko 改进动态认证协议存在的问题

Lee-Chun Ko 的方案[7]通过对时延的严格控制和对

收稿日期:2012-02-13;修回日期:2012-05-31
基金项目:国家自然科学基金(No.61172053,No.61003234,No.U0835004);北京市自然科学基金(No.4102012);国家 863 高技术研究发展计划(No.2012AA011706)

认证通过信息的签名方式解决了 Wong 和 Tseng 方案中的不足,但由于这一方案在每一个登录节点上都分配了 N 这一重要信息,一旦这一信息泄漏,将导致重大的安全问题.同时由于每一个登录节点都要保存所有用户的 N,将导致安全威胁的扩大.

2　动态用户认证协议的分析与改进

上述协议都保留了低消耗和高效的特点,但是由于上述方案都依赖于网关,网关成为上述协议的一个重要安全瓶颈.因此动态用户认证协议的改进还需要同时从网关和协议两个方面入手.

2.1　设计思想

为了确保网关的安全瓶颈得到保证,我们提出了一种基于虚拟机技术的无线传感器网络的网关结构[8],其设计结构图如图 1 所示.

基于该模型,提出了动态用户认证协议的改进方案.在不影响其高效的前提下,提高了安全性,增强了对伪装网关重放攻击和针对网关的拒绝服务攻击的安全性.

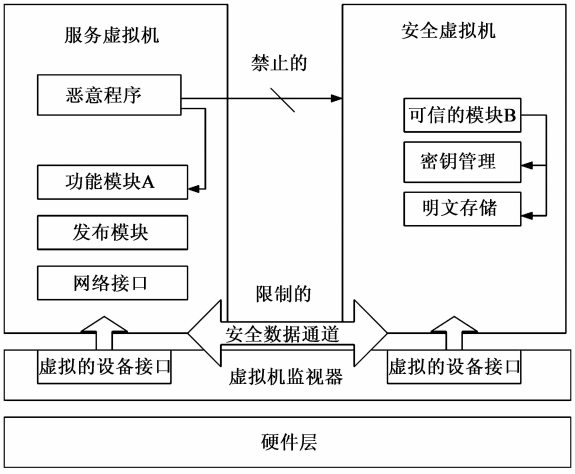

图1　基于虚拟机技术的网关模型

2.2　改进的动态用户认证方案

改进的动态用户认证方案包括以下阶段:

2.2.1　注册阶段

(1)用户拥有 UID,选择口令 PW.通过安全信道向网关提交 $(UID, hash(PW))$;

(2)网关在数据库中存储 $(UID, T, hash(PW), TS)$,并向各登录节点用安全方式分发其子集 (UID, T, TS),其中 TS 为有效时戳,T 为最近一次的登录时间,初始化为用户注册时刻;

(3)网关通知用户注册成功.

2.2.2　登录阶段

(1)用户计算

$$A = hash(hash(PW) \oplus t_1)$$

之后向登录节点提交登录信息 (UID, A, t_1),其中 t_1 为当前时刻;

(2)登录节点检查 UID 是否存在,若不存在向用户发送 UID 错误消息 $Msg(ID\_WRONG)$.如 UID 存在,检查是否 $\Delta t < t_1 - T$,其中 Δt 为最小有效登录间隔,如果登录时间差小于 Δt,则证明用户登录频繁,将请求弃置,拒绝用户登录;否则判断 $t_c - t_1$ 是否超过最大传输时延,t_c 为当前时刻,检查是否超时.超时则发送超时 $Msg(OVERTIME)$ 消息,拒绝用户登录.否则进行以下计算:

$$C = hash(A \oplus t_2)$$

$$D = hash(UID \oplus S \oplus C)$$

其中 S 为登录节点与网关的共享秘密,不同的登录节点的 S 不同.t_2 为进行计算时的当前时刻.修改 $T = t_1$.之后登录节点向网关提交 (UID, C, D, t_1, t_2).

2.2.3　认证阶段

(1)网关检查 (UID, t_1) 是否存在,即检查用户是否已经登录,如 (UID, t_1) 已经存在,则弃置这一认证请求.检查是否 $\Delta t < t_1 - T$,并判断 $t_c - t_2$ 是否超出最大传输时延,如果登录频繁或者超过时延,则弃置这一认证请求.如不超时依照式(1)进行如下计算:

$$D' = hash(A \oplus S \oplus C) \tag{1}$$

并判断 D' 是否和 D 相等,如不相等认为登录节点为伪装或登录节点出错,拒绝登录,不发送任何信息,并在收到此类包达到一定阈值时启动对节点中恶意节点的排除.否则依照式(2)(3)继续计算

$$A' = hash(hash(PW) \oplus t_1) \tag{2}$$

$$C' = hash(A' \oplus t_2) \tag{3}$$

判断与 C' 与 C 是否相等,如不相等发送拒绝登录消息,否则认为用户认证成功.网关保存 $T = t_1$,计算网关对消息的签名:

$$MA_{sn} = hash(A \oplus S \oplus t_4)$$

$$MA_u = hash(A \oplus hash(PW))$$

之后网关向登录节点发送接受认证消息

$$(Msg(ACC\_LOGIN), MA_{sn} \oplus MA_u, hash(MA_u), t_4)$$

(2)登录节点首先检查 $t_c - t_4$ 是否超过最大传输时延,t_c 为当前时刻.如超时,则放弃这个包.如不超时则依照式(4)首先计算

$$MA'_{sn} = hash(A \oplus S \oplus t_4) \tag{4}$$

之后计算 $MA'_u = MA_{sn} \oplus MA_u \oplus MA'_{sn}$ 并验证是否 $hash(MA_u) = hash(MA'_u)$,验证失败则认为消息为伪造,不做处理.否则向登录用户发送:

$$(Msg(ACC\_LOGIN), hash(MA_u \oplus t_5), t_5);$$

如登录节点收到拒绝登录消息,同样首先计算是否超时,如不超时则计算验证 $h(MA_{sn}) = h(MA'_{sn})$,如正确则

发送拒绝登录消息给用户:

$$(Msg(REJ\_LOGIN), hash(MA_u \oplus t_5), t_5)$$

(3)用户接受来自登录节点的登录消息并验证

$$hash(MA_u \oplus t_5) = hash(hash(A \oplus hash(PW)) \oplus t_5)$$

如验证成功,则接受登录节点的通知.

2.2.4 更新阶段

(1)用户产生新的口令 PW',并通过当前安全通道向网关提交

$$[UID, hash(hash(PW')), hash(hash(PW)), hash(PW) \oplus hash(PW')]$$

(2)网关根据自己储存的用户口令哈希值判断 $hash(hash(PW))$是否正确后计算

$$hash(PW'') = hash(PW) \oplus hash(PW') \oplus hash(PW)$$

如 $hash(hash(PW'')) = hash(hash(PW'))$,则认为发送正确,将 $hash(PW'')$作为新的用户口令哈希存储,并按照注册阶段进行操作.

2.3 网关登录消息的格式

在之前的动态用户认证协议中,没有对网关发送给登录节点的允许登录消息 $Msg(ACC_LOGIN)$和拒绝登录消息 $Msg(REJ_LOGIN)$的具体格式给出说明.通过之前对于协议的分析可以知道,用户实际上接入无线传感器网络最终是依靠登录节点的.因此网关的登录消息必须保证不能被伪造,否则如果攻击者可以对某一登录节点进行控制,那么他可以不通过网关进行认证,让控制的登录节点直接伪造登录消息,让用户通过认证.鉴于以上分析,应当对协议中的网关的登录消息给出一种具体格式.

为了使登录消息无法被伪造,本文借鉴了 μTESLA 协议使用单向密钥链的方式保证登录消息不能被伪造.

假设无线传感器网络内部共享单向密钥生成函数 $f(x)$,M 为密钥链长度,对初始密钥 K 进行计算,保证对于任意的密钥 K_{i+1},其子密钥 $K_i = f(K_{i+1})$.进行 M 次运算产生密钥链 $f^{(0)}(K), f^{(1)}(K), f^{(2)}(K), \cdots\cdots, f^{(M)}(K)$,$f^{(M)}(K)$对应 K_0.

当网关完成用户认证时产生登录消息,其格式如表 1 所示.其中 P(permission)表示用户的权限,可以表示是否对用户认证成功;T_{BEGIN} 和 T_{END} 分别表示网关产生这条消息的时间,和这条消息失效的时间,可以保证消息的新鲜性;K_{n-1} 为上次使用的密钥;MAC 使用 K_n 计算.

登录节点在收到来自网关的登录消息后首先根据上节的步骤判断消息是否来自网关,如果成功,则将登录消息广播给范围内的节点.节点每次收到消息后可以根据 $K_{n-2} = f(K_{n-1})$检查上次收到的消息是否来自网关,如果验证出错,则认为登录节点欺骗,否则根据消息做出相应的许可或者禁止操作,并记录 K_{n-1} 和 MAC 值,在收到下次消息时检查登录节点是否欺骗.

表 1 网关登录消息格式

用户标志	权限	开始时间	结束时间	前次密钥	使用当前密钥计算的 MAC 值
UID	P	T_{BEGIN}	T_{END}	K_{n-1}	$MAC(K_n, UID \mid permission \mid T_{BEGIN} \mid T_{END} \mid K_{n-1})$

3 改进的动态用户认证方案的性能分析

以 Lee-Chun Ko 为基础的动态用户认证协议经过改进后,在保证认证方案高效的前提下提高了安全性,特别是对以下攻击的防御性能有了大幅度提高.

3.1 伪装网关重放攻击防御

伪装网关重放攻击,主要是由于无线传感器网络节点易于被捕获的特点,以及原协议设计的不合理,导致任意登录节点被捕获后,使攻击可以发生.即使通过相应的协议可以将捕获的登录节点排除,攻击者依然可以在 Lee-Chun Ko 的方案中通过其他登录节点登录.因此在修改协议中没有使用通用的 N 值,而是使用了每个登录节点与网关的一个共享秘密 S,防止节点捕获后的影响扩大.同时通过使用 S 参与网关的签名,保证了攻击者无法伪装网关重放认证消息.

当攻击者试图使用伪装网关重放攻击时,假设攻击者捕获了某一登录节点,并获得了相应的 S,同时此节点被通过排除恶意节点的方式排除.恶意攻击者使用 UID 和伪造的 A 登录,当前登录节点使用(UID, CD, t_1, t_2)登录,其中

$$C = hash(A \oplus t_2) \tag{5}$$

$$D = hash(UID \oplus S' \oplus C) \tag{6}$$

此时,攻击者可以阻塞登录节点信息的提交.但是由于攻击者不知道有关 S' 的任何消息,因此无法通过式(7)

$$MA_{sn} = h(A \oplus S' \oplus t_4) \tag{7}$$

伪造 MA_{sn},无法伪造($Msg(ACC\_LOGIN)$, $MA_{sn} + MA_u$, $hash(MA_u)$, t_4),无法伪装网关重放攻击.

如果攻击者尝试通过被捕获的登录节点进行登录时,由于攻击者不知道用户 UID 对应的 $hash(PW)$值,因此无法计算出正确的 A 值,因此,无法通过式(5)和式(6)计算出正确的 C 和 D,因此无法通过网关的认证.

当攻击者尝试使用被捕获的登录节点伪造网关登录消息,试图直接认证用户时,由于登录消息格式的原因,攻击者无法计算出单向密钥链中下一个密钥,因此伪造登录消息.即使攻击者通过修改消息内容方式欺

骗登录后,在下一次登录消息到来时,节点就可以发现登录节点的欺骗,进而将登录节点和恶意用户排除出网络.

3.2 拒绝服务攻击的防御

针对于拒绝服务攻击,由于在登录节点部分对用户的登录频率做出了限制,攻击者不能通过登录节点实施拒绝服务攻击.而在此方案中每个登录节点都与网关共享秘密 S,而在登录阶段中,登录节点需要提交由 S 构造的 D,网关可以通过检查 D 是否正确,判断认证消息是否来自正确的登录节点,减小了网关判断的计算量,对于假冒登录节点的针对网关的拒绝服务攻击也很有效.

同时,在方案中,限制了同一 UID 的登录间隔.每当登录请求到来时,登录节点或者网关检查此用户上次登录到当前时刻的时间间隔,防止登录过于频繁,以此减小重复发送同一 UID 假认证包的拒绝服务攻击的可能.

如果没有这种方式,网关很可能被拒绝服务攻击方式攻击.而正常用户不可能频繁登录网络,因此这一功能的添加可以提高协议抵抗拒绝服务攻击的能力.同时是节点在向网关提交认证请求时,需要发送 D,由于 D 是由网关和登录节点共享的秘密 S 参与产生的,可以保证此请求由相应的登录节点产生,也在一定程度上防止了恶意节点伪装登录节点进行更换的 UID 方式的拒绝服务攻击.

在这种攻击方式中恶意节点不断更换 UID,伪装登录节点对网关进行拒绝服务攻击.在 Lee-Chun Ko 的协议中网关在完成基本的检查之后需要进行以下运算:

$$A^* = hash(hash(PW) \oplus t_1)$$

$$C^* = hash(A^* \oplus hash(N \oplus t_3))$$

并验证是否 $C = C^*$.此时由于 $C \neq C^*$ 拒绝登录,并向登录节点发送 $Msg(REJ\_LOGIN)$.

而在使用上一节改进的协议后,只需要进行运算

$$D' = hash(A \oplus S \oplus C)$$

由于攻击者无法产生合适的数据,所以 $D \neq D'$.此时网关认为认证包虚假将请求包弃置,节省了很大的计算量.表 2 中对两种认证方式的计算量作出了比较,其中 X 为一次异或运行,H 为一次哈希运算.可以看出,改进协议比 Lee-Chun Ko 的协议检验到登录失败需要的运算更少.但是因为原有协议在拒绝登录信息中没有签名,因此原协议如果在拒绝登录消息上加入签名运算,实际的运算量更大.

而且由于当这些包的数量在一定时间范围内到达阈值时,网关认为收到拒绝服务攻击.当发现了拒绝服务攻击时,可以进行相关的防御措施[9].

表 2　两种协议判断恶意登录计算量比较

	Lee-Chun Ko 的协议	改进的协议
进行的运算	$3X + 3H$	$2X + H$

3.3 协议的其他特性

修改的协议除了对上述攻击的有效抵抗外,还具有以下特性.

(1)伪装网关的登录拒绝攻击通过使用在拒绝登录的消息中加入签名的方式而避免;

(2)协议修改了更新阶段,使更新过程可以在不安全的信道下完成.即口令的更新可以在无线传感器网络内进行,口令的更新更加方便;

(3)协议依然保持了动态用户认证协议轻量级高效的特点,表 3 列出了登录和认证阶段的时间,其中 T_x 为进行异或运算需要的时间,T_h 是进行一次单向哈希函数需要的时间,T_t 为登录节点和网关间一次多跳传输的时间.

表 3　两种协议运行时间的比较

	Lee-Chun Ko 的协议	改进型的协议
登录阶段	$3T_x + 3T_h + 1T_t$	$4T_x + 3T_h + 1T_t$
认证阶段	$13T_x + 10T_h + 1T_t$	$14T_x + 11T_h + 1T_t$
总计	$16T_x + 13T_h + 2T_t$	$18T_x + 14T_h + 2T_t$

通过上表中两种协议在进行一次用户认证过程中所需的时间比较,我们可以看出.改进型协议保留了原协议轻量级、快速认证的特点.通过上图可以看出改进型协议在一次用户认证过程中所用的总时间略多于 Lee-Chun Ko 提出的协议.但考虑到改进协议中对原协议安全强度的提升,在认证过程中产生的时间代价是可以接受的.

4 小结

本文分析了无线传感器网络主要的动态协议的特点及存在的安全隐患.针对存在问题提出了一套包括网关和协议改进的解决方案,该方案针对网关安全引入了基于虚拟机技术的具有一定安全隔离性的网关结构.结合该网关结构对用户动态协议进行了改进.经分析,改进的协议保持了原协议高效低耗的特性并提高了其安全性和便利性.

参考文献

[1] 周贤伟,施德军,覃伯平.无线传感器网络认证机制的研究[J].计算机应用研究,2006,12:108 – 111.
Zhou Xian-wei, Shi De-jun, Zhang Bo-ping. Research on authentication strategy in wireless sensor network[J]. Application Research of Computers, 2006, 12: 108 – 111. (in Chinese)

[2] 李中献,詹榜华,杨义先.认证理论与技术的发展[J].电子学报,1999,26(1):99 – 103.
Li Zhong-xian, Zhan Bang-hua, Yang Yi-xian. A survey of identification and authentication[J]. Acta Electronica Sinica, 1999,26(1):99 – 103.(in Chinese)

[3] Kirk H M Wong, Yuan Zheng, Jiannong Cao. A dynamic user authentication scheme for wireless sensor networks[A]. Proceedings of the IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing[C]. SUTC, 2006.244 – 251.

[4] C Y Lee, C H Lin, C C Chang. An improved low communication cost user authentication[A]. Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications[C]. Taiwan: AINA, 2005.249 – 252.

[5] H R Tseng, R H Jan, W Yang. An improved dynamic user authentication scheme for wireless sensor networks[A]. Proceedings of the IEEE Global Communications Conference[C]. GLOBECOM, 2007.986 – 990.

[6] Binod Vaidya, Jorge Sá Silva, Joel J P C Rodrigues. Robust dynamic user authentication scheme for wireless sensor networks[A]. Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks[C]. Spain: ACM, 2009.28 – 29.

[7] Lee-Chun Ko. A novel dynamic user authentication scheme for wireless sensor networks[A]. IEEE International Symposium on Wireless Communication Systems[C]. 2008.608 – 612.

[8] 裴庆祺,宁奔,吴洋,杨亮,尹浩,唐宏.基于虚拟机的异构环境下无线传感器网络网关设计[J].网络安全技术与应用,2011,6:5 – 8.
Pei Qing-qi, Ning Ben, Wu Yang, Yang Liang, Yin Hao, Tang Hong. Gateway of wireless sensor network based on VM in heterogeneous environment[J]. Network Security Technology & Application, 2011,6:5 – 8.(in Chinese)

[9] Zhen Cao, Xia Zhou, Maoxing Xu. Enhancing base station security against QoS attacks in wireless sensor networks[A]. Wireless Communications, Networking and Mobile Computing 2006 International Conference[C]. Wuhan: IEEE, 2006.1 – 4.

作者简介

刘 云 男,1981 年 7 月出生于重庆市忠县.2006 年毕业于电子科技大学通信学院,硕士学位,现为在读博士.主要从事计算机网络,无线网络及信息安全方面的研究.
E-mail: cloud_ly@163.com

王 勇 男,1964 年 3 月出生于四川.2005 年 6 月毕业于华东理工大学,博士学位,现任国家软件与集成电路公共服务平台广西分中心常务副主任.主要从事网络信息安全等方面的研究.

杨 亮 男,1986 年 3 月出生于河北承德.2011 年毕业于西安电子科技大学,硕士学位,现为中兴通信股份有限公司软件工程师.主要从事物联网和移动通信方面的研究.

唐仕军 男,1985 年 6 月出生于广西桂林.2009 年毕业于桂林电子科技大学,学士学位,现于桂林电子科技大学就读硕士研究生.主要从事智能信号处理等方面的研究.

范科峰 男,1978 年出生于陕西礼泉.2009 年毕业于西安电子科技大学,博士学位,中国电子学会高级会员,IEC TC100 DRM 及 JTC1 DCMP 专家.主要从事无线网络及信息安全方面的研究.