

文章编号:1001-9081(2014)02-0452-04

doi:10.11772/j.issn.1001-9081.2014.02.0452

基于改进 Das 协议的无线传感器网络用户认证协议 UAPL

万智萍*

(中山大学 新华学院, 广州 510520)

(*通信作者电子邮箱 wzp888_0@126.com)

摘要:针对在无线传感器网络中采用用户认证的方式获取节点数据时,容易出现密码被破译,以及容易遭受多种网络攻击等安全性问题,在改进 Das 协议的双因素身份验证的基础上,引入了用户与网关、网关与传感器节点之间的互相验证机制以及用户密码变更机制,提出了 UAPL 协议。UAPL 协议具有防止网关节点旁路攻击、伪装攻击等网络攻击的安全验证机制,提供的密码变更防护能防止由于密码泄露而引发的安全问题。实验结果表明,UAPL 协议与其他改进 Das 协议相比具有较高的安全性。

关键词: 用户认证协议; Das 协议; 互相验证机制; 密码变更机制; 网络攻击

中图分类号: TN918.1 **文献标志码:**A

UAPL: Wireless sensor network user authentication based on improved Das protocol

WAN Zhiping*

(Xinhua College of Sun Yat-sen University, Guangzhou Guangdong 510520, China)

Abstract: When obtaining node data through user identification in wireless sensor networks, passwords may be cracked and some other security problems such as being prone to network attacks may occur. Concerning these problems and based on the improved Das' protocols of two-factor user authentication, UAPL protocol was proposed after introducing a verification mechanism between users and gateway nodes as well as between gateway nodes and sensor nodes, and a mechanism for changing's password. This protocol had security features that prevented gateway node sideway attacks, masked attacks and other network attacks and its provided capability of password change protection could prevent security problems when passwords were leaked out. The experimental results show UAPL protocol offers much higher security than other improved Das' protocols.

Key words: user authentication protocol; Das agreement; mutual authentication mechanism; password change mechanism; network attack

0 引言

无线传感器网络在工业、民用和军事上都被广泛应用,因此一旦网络被恶意攻击,有可能造成信息泄露、重要数据丢失,以及用户密码被篡改等严重问题,尤其在工业和军事应用上,一旦无线传感器网络中的重要数据被攻击者所获取,会造成非常大的经济损失和安全威胁^[1-2]。无线传感器网络安全的研究领域之一是用户身份验证方案^[3-4],允许唯一真实身份的用户访问由传感器节点采集到的数据。能否设计一种用户认证协议,有效防止网络攻击者篡改用户密码或利用漏洞获取节点数据信息是本文的研究重点。

Das^[5]提出了双因素用户认证协议的无线传感器网络,填补了传统用户认证协议存在的漏洞,并建立起会话密钥,一定程度上提高了用户认证效率。Chen 等^[6]指出 Das 协议在无线传感器网络上,网关节点和传感器节点之间相互认证协议存在的一个安全漏洞。为了解决此问题,他们提出了一个具有保密性的改进的 Das 协议,确保了合法用户在存在网络攻击的环境中仍能保持一定的安全性。Khan 等^[7]指出,在 Das 协议中用户不能更改/更新自己的密码,而且它不提供网关节点和传感器节点之间的相互认证,导致网关节点在遭受

旁路攻击和内部特殊攻击时是脆弱的,为此他们提出了改进方案和安全补丁程序,修复 Das 协议的脆弱部分。He 等^[8]提出提出了隐私保护数据聚合(Privacy Data Aggregation, PDA)的无线传感器网络,采用了一个非树状拓扑结构保护各个节点的数据隐私,并提出了两个方案:1) 基于集群的私人数据聚合(Cluster-based Private Data Aggregation, CPDA);利用多项式的聚类协议和代数性质。2) 切片混合聚合(Slice-Mix-AggRegaTe, SMART):建立在切片技术上并联合其他属性。在文献[6]中提出的改进 Das 协议仍然存在不足,例如在并行对话遭遇和内部特殊攻击时安全机制存在漏洞,且不提供更改密码机制。文献[7]提出的 Das 协议的改进方案在处理并行会话攻击时存在漏洞,而且在防止网关节点旁路攻击时只提供部分的保护。

相比缺少互相验证机制和密码变更机制的 Das 协议,本文提出了 UAPL 协议,在协议的注册阶段、认证识别阶段都加强了安全防护,从用户发送查询请求到传感器节点响应请求的过程中,通过生成密匙、秘密参数和计算哈希函数进行双向验证。UAPL 协议的安全验证机制相比其他改进 Das 协议,可以防止攻击者通过伪装的传感器节点破译网关节点发送的验证值,以及防止攻击者通过蛮力攻击来破译用户密码。

收稿日期:2013-08-09 ;修回日期:2013-10-17。

作者简介:万智萍(1980 -),男,湖北鄂州人,讲师,硕士,主要研究方向:目标跟踪、图像处理、机器学习、无线传感器网络、网络物理系统。

1 相关工作

1.1 Das 协议

Das 协议是由 Das 在 2009 年提出的一种无线传感器网络用户认证协议^[9],协议主要使用双因素身份验证的方法,可以防止其他的用户使用相同的登录身份,以及进行被盗验证和防止伪装、重放威胁等。Das 协议由注册阶段、登录阶段和账号验证阶段组成,主要的用户认证处理过程^[9]如下。

注册阶段 假设用户 i 使用一个安全的信道来提交自己的账号(Identification) ID_i 和密码(Password) PW_i 到网关节点(Gateway node) n_w ,在网关节点 n_w 将利用哈希(Hash)函数 $H(key)$ ^[10] 来计算,计算值 DZ 作为该账号和密码的存储地址,表示为:

$$DZ = H(ID_i \parallel PW_i) \oplus H(key)$$

其中: key 表示对称密匙(Symmetric Key), \parallel 是一个串联运算符。 $H(\cdot)$ 表示一个哈希函数。得到 DZ 的值后,一个秘密参数 ξ_a 通过网关节点 n_w 生成并存储在传感器节点中,且网关节点 n_w 会利用计算值 DZ 、密码的存储地址 $H(PW_i)$ 和账号 ID_i 使用用户的智能卡的参数个人化,使用户在使用智能卡进行身份验证时安全性更强。

登录阶段 用户 i 使用智能卡插入到终端,并输入自己的 ID_i 和 PW_i ,通过智能卡存储的数据确定用户登录的账号为有效信息时,就会开始通过账号和密码信息计算验证信息 DID_i 和 C_i :

$$DID_i = H(ID_i \parallel PW_i) \oplus H(\xi_a \parallel TP)$$

$$C_i = H(DZ \parallel \xi_a \parallel TP)$$

其中, TP (Timestamp) 指用户在整个登录阶段的当前时间截。得到 DID_i 和 C_i 的值后,发送验证信息集 $\{DID_i, C_i, TP\}$ 到网关节点 n_w 。

验证阶段 当网关节点在 TP_n 时刻收到登录请求时,就会对 TP 进行时间验证。如果出现 $TP_n - TP > t$, t 表示允许的最大通信延迟,则网关节点会中断验证处理。当网关节点没有中断验证处理时,就会计算存储地址 $H(ID_i \parallel PW_i)^*$ 和验证信息 C_i^* 的值:

$$H(ID_i \parallel PW_i^*) = DID_i \oplus H(\xi_a \parallel TP)$$

$$C_i^* = H((H(ID_i \parallel PW_i)^* \oplus H(key)) \parallel \xi_a \parallel TP)$$

当验证信息 C_i 不同于 C_i^* ,则网关节点拒绝登录请求,若两个值相同,则 n_w 会发送验证信息集 $\{DID_i, A_i, TP'\}$ 到最近的传感器节点(Sensor node) n_j 去响应数据查询请求。其中 A_i 表示来自合法的网关节点的验证信息,由秘密参数 ξ_a 生成, A_i 的计算公式为: $A_i = H(DID_i \parallel n_j \parallel \xi_a \parallel TP')$, TP' 指当前网关节点 n_w 在验证阶段的当前时间截。节点 n_j 首先对 TP' 进行验证,当不超过允许的最大通信延迟时,计算 $H(DID_i \parallel n_j \parallel \xi_a \parallel TP')$ 的值是否等于 A_i ,若相等,节点 n_j 响应用户 i 查询传感器数据的要求。

1.2 改进 Das 协议

Das 协议提出后,近年来有许多学者对 Das 协议进行了研究和改进。Khan 等^[11]发现 Das 协议容易遭受网关节点旁路攻击和内部特殊攻击,安全性存在一定缺陷,因此针对发现的问题对 Das 协议进行了改进;但 Khan 改进后的协议缺乏用户与网关节点之间的互相验证机制,而传感器网络提供远程

管理/查询功能允许用户访问来自远程终端的网络数据,当非法用户使用伪造的网关节点收集网络数据时,由于缺乏互相验证机制将导致网络数据容易被非法获取。Nyang-Lee 等^[12]分析了 Das 协议在遭受密码猜测攻击和网关节点模拟攻击时的脆弱性,提出了一种增强 Das 协议安全性的协议;但该协议缺乏用户密码更改机制,当用户的密码泄露后,将无法修改之前设定的密码,存在极大的安全隐患。Chen 等^[13]在对 Das 协议的研究中提到该协议在用户和网关节点之间缺少互相认证,并且在遭受并行会话攻击时有一定的脆弱性,因此针对 Das 协议的改进从而提出了一种鲁棒性更好的基于相互认证协议的无线传感器网络;但网络不能很好地防范传感器节点的欺骗攻击,当非法用户放置一个假的传感器节点并利用假数据去响应验证信息集 $\{DID_i, A_i, TP'\}$ 时,网关节点无法识别假数据并认定数据是否有效,这样的一个漏洞会危机整个网络的安全。

2 UAPL 协议

2.1 注册防护

在一个传感器网络中,为了使用传感器节点所采集到的数据,合法用户 i 会通过注册的方式来获得一个合法账号。假设一个用户选择的账号为 ID_i ,密码为 PW_i ,并将它们输入到网络终端,网络终端将产生一个随机数(Random number) a_i ,并得到计算值 PS_i :

$$PS_i = H(PW_i) \oplus a_i$$

其中: $H(PW_i)$ 是一个哈希函数, \oplus 是异或运算符。得到 PS_i 的值之后,账号 ID_i 和密码为 PW_i 通过安全信道被发送至网关节点。网关节点接着计算验证信息:

$$B_i = H(ID_i \parallel PS_i)$$

$$P_i = H(ID_i \parallel PS_i) \oplus H(key \parallel \xi_a)$$

$$R_i = H(\xi_a \parallel ID_i)$$

其中: key 指通过网关节点唯一已知的对称密匙, ξ_a 是由网关节点产生的秘密参数, \parallel 是串联运算符。当验证信息 B_i 、 P_i 、 R_i 被计算出来时, B_i 、 P_i 、 R_i 和 $H(ID_i \parallel PS_i)$ 使用用户智能卡的参数个人化,并且网关节点存储 a_i 到智能卡中。同时,独立的密匙 $key(n) = H(\xi_a \parallel n_i)$ 被存储在每个传感器中负责与用户交接数据, n_i 为传感器节点的标识。

2.2 认证识别防护

当用户请求访问传感器节点的数据时认证识别防护开始执行,分为登录和验证阶段。在登录阶段,用户插入自己的智能卡,并输入 ID_i 和 PW_i ,此时智能卡开始计算:

$$PS_i = H(PW_i) \oplus a_i$$

$$B_i^* = H(ID_i \parallel PS_i)$$

得到验证信息 B_i^* 后进行用户身份验证,如果验证信息 B_i^* 与 B_i 值不匹配,认证请求被拒绝;两个值匹配时,智能卡继续计算:

$$DID_i = H(ID_i \parallel PS_i) \oplus H(key_i \oplus TP)$$

TP 是用户在当前阶段的时间截,在用户的认证请求通过的同时生成一个随机的新鲜值 N_i ,得到 DID_i 值之后发送验证信息集 $\{DID_i, TP, ID_i, N_i\}$ 到网关节点。

在验证阶段,网关节点在 TP^* 时刻接收到登录请求时,开始验证 TP 是否满足 $(TP^* - TP) \leq t$ (t 指允许的最大通信

延迟),若满足,则网关节点计算:

$$\begin{aligned}key_i^* &= H(\xi_a \parallel ID_i) \\H(ID_i \parallel PS_i)^* &= DID_i \oplus H(key_i^* \parallel TP) \\M_i &= H(H(ID_i \parallel PS_i)^* \parallel key_i^* \parallel N_i)\end{aligned}$$

key_i^* 指 TP^* 时刻通过网关节点唯一已知的对称密匙。得到验证信息 M_i 后,网关节点生成一个随机新鲜值 N_i^* 并发送信息 $\{M_i, N_i^*\}$ 到用户智能卡,智能卡开始计算:

$$M_i^* = H(B_i \parallel key_i \parallel N_i)$$

并验证 M_i^* 与 M_i 是否相同,相同时网关节点生成一个随机新鲜值 (Random value fresh) N_{ii} 并发送验证信息集 $\{DID_i, TP'_i, N_{ii}\}$ 到一些较近的传感器节点 n_j 响应用户的查询数据请求, TP' 指网关节点发送消息时的当前时间戳。收到信息的传感器节点 n_j 开始验证 $TP'_i - TP^* \leq t$ 是否成立,成立时继续计算:

$$G_i = H(key_n \parallel TP'_i \parallel N_{ii})$$

并发送信息 $\{G_i, N_n\}$, N_n 是传感器节点 n_j 生成的一个随机新鲜值。得到 G_i 后网关节点计算:

$$\begin{aligned}key_n^* &= H(\xi_a \parallel n_j) \\G_i^* &= H(key_n^* \parallel TP'_i \parallel N_{ii})\end{aligned}$$

当 $G_i^* = G_i$ 时,传感器节点 n_j 发送信息 $\{W_i\}$ 使网关节点响应 n_j 的查询允许,其中 $W_i = H(DID_i \parallel key_n^* \parallel N_n)$ 。当网关节点收到节点 n_j 发送的信息时,开始计算验证信息:

$$W_i^* = H(DID_i \parallel key_n \parallel N_n)$$

当 $W_i^* = W_i$ 时,用户可以成功地查询传感器节点 n_j 的数据。

会话密匙建立。一个密匙在用户智能卡端和网关节点之间表示为:

$$key_1 = H(N_i \parallel N_{ii} \parallel key_i)$$

在网关节点和收集数据的传感器节点 n_j 之间表示为:

$$key_2 = H(N_n \parallel N_{ii} \parallel key_n)$$

当在智能卡端和节点 n_j 之间需要一个通信信道,一个双边会话密匙通过网关节点建立:

$$key_{12} = H(N_{ii} \parallel key_i \parallel key_n)$$

此时,网关节点生成一个随机值 key_{12} 并发送 $N_i \parallel key_{12}$ 加密 key_1 到智能卡端,且 $N_n \parallel key_{12}$ 加密 key_2 到传感器节点 n_j 一端。

2.3 密码变更防护

当用户需要变更密码时,在插入智能卡后输入自己原先的账号 ID_i 和密码 PW_i ,等待登录和认证成功后,输入新的密码 (New Password) NPW_i ,智能卡开始计算:

$$\begin{aligned}PS_i &= H(PW_i) \oplus a_i \\B_i^* &= H(ID_i \parallel PS_i)\end{aligned}$$

验证信息 B_i^* 与 B_i 之间是否匹配,匹配时密码更改请求通过,用户输入新密码,智能卡开始计算验证信息 NB_i 、 NP_i 和密匙的存储地址 $H(key \parallel \xi_a)$:

$$\begin{aligned}NB_i &= H(ID_i \parallel NPS_i) \\H(key \parallel \xi_a) &= P_i \oplus H(ID_i \parallel PS_i) \\NP_i &= H(ID_i \parallel NPS_i) \oplus H(key \parallel \xi_a)\end{aligned}$$

其中计算值 $NPS_i = H(NPW_i) \oplus a_i$,智能卡通过 NB_i 、 NP_i 代替 B_i 、 P_i ,完成密码更改操作。

3 应对多种网络攻击的安全验证

对于可能发生的网络攻击情况,假设攻击者可以拦截用户在智能卡终端、网关节点、采集到数据的传感器节点 n_j 这三者之间传达的所有信息,并假设用户的智能卡已被攻击者盗取,在这种情况下,攻击者会采取多种可能的攻击计划。

3.1 网关节点旁路攻击

网关节点旁路攻击是指攻击者通过网关节点绕过对加密算法的繁琐分析,取得在运算中泄露的秘密参数,并得到 DID_j :

$$\begin{aligned}DID_j &= H(ID_j \parallel PW_j) \oplus H(\xi_a \parallel TP_j) \\M_j &= H(DID_j \parallel n_j \parallel \xi_j \parallel TP_j)\end{aligned}$$

在 UAPL 协议中智能卡和传感器节点 n_j 并不存储秘密参数 ξ_a 和 ξ_j ,而是存储在密匙中:

$$\begin{aligned}key_i &= H(\xi_a \parallel ID_i) \\key_n &= H(\xi_a \parallel n_j)\end{aligned}$$

因此传感器节点 n_j 和智能卡具有唯一性,即攻击者只能获取当前智能卡的持有者在传感器节点 n_j 所拥有的数据,该节点存储的其他用户的数据不会被攻击者同时获取,而且其他传感器节点不受影响。

3.2 伪装攻击

攻击者放置一个自己伪装的传感器节点来冒充无线传感器网络的正常节点,以达到获取 DID_i 和 M_i 的目的。在 UAPL 协议中这两者都是通过单向哈希函数进行计算:

$$\begin{aligned}DID_i &= H(ID_i \parallel PS_i) \oplus H(key_i \parallel TP) \\M_i &= H(H(ID_i \parallel PS_i)^* \parallel key_i^* \parallel N_i)\end{aligned}$$

由于验证信息 DID_i 、 M_i 都是通过秘密值来求出,因此攻击者无法破译。

3.3 猜测攻击

在 UAPL 协议里,明文中的秘密值不会发送到节点,而是在一个单向散列函数里被加密。因此,即使攻击者得到了 DID_i 、 M_i 、 B_i ,由于哈希函数的单向属性使攻击者也无法猜出任何秘密值 $\{PW_i, key_i, key_n, key\}$ 。而且本文协议基于智能卡计算和用户密码这种双因素认证的方法相比只基于密码认证的协议,具有更高的安全性。

3.4 蛮力攻击

攻击者可以通过在认证识别阶段发送由 DID_i 和 M_i 或 DID_i 和 W_i 组合的序列信息至网关节点或存储数据的传感器节点来强行破译用户身份验证操作,但在 UAPL 协议中,每个身份验证过程都使用不同的随机数,这样使得身份验证被破译的概率极低,安全性也得到较大增强。另一方面,攻击者可能会通过尝试不同的秘密值 key 和秘密参数 ξ_a 来进行破译,但在 UAPL 协议中,额外的随机数 R_i 和 R_D 可以被添加于秘密值 key_i 中:

$$\begin{aligned}key_i &= H(\xi_a \parallel ID_i \parallel R_i) \\key_n &= H(\xi_a \parallel n_j \parallel R_D)\end{aligned}$$

这样攻击者破译 key_i 和 key_n 时需要尝试的可能的组合数就增加了 2^{R_i} 倍和 2^{R_D} 倍,破译的难度将变得更高,这样有效地加强了网络数据的安全性。

4 性能分析

表 1 为 UAPL 协议与其他改进 Das 协议的安全特性对比

结果,从表中可以看出,除了 UAPL 协议外,另外三个协议都不具有防护传感器节点节点伪装攻击以及防护蛮力攻击的安全特性。

而且除了 UAPL 协议和 Nyang-Lee^[12]提出的协议外,其他两个协议都没有实行智能卡与网关的相互验证操作。

表1 安全特性比较

安全特性	UAPL 协议	Khan-Alghathbar 协议	Nyang-Lee 协议	Chen-Shih 协议
安全密码更改服务	是	是	否	否
防护网络节点旁路攻击	是	是	是	否
防护伪装攻击	是	否	否	否
防护猜测攻击	是	是	是	否
防护蛮力攻击	是	否	否	否
智能卡与网关相互验证	是	否	是	否
网关与其他节点相互验证	是	是	是	否

参考文献[11~13]的实验方法,本文比较 UAPL 协议与相关的 Das 改进协议在注册、登录、验证、密码变更阶段中的计算成本,因为这些阶段的程序是用户认证协议中的主要部分。本文定义 T 为哈希函数的计算时间, T_1 作为私有密钥计算时间, T_2 作为公共密钥的计算时间,其中 $T_1 \gg T, T_2 \gg T$ 。协议的运行结果示于表 2 中。哈希函数需要的计算时间远比公共和私有密匙的计算时间少,因为公共密匙和私有密匙需要多项式计算的时间成本。因此 Nyang-Lee^[12]提出的协议相

比其他协议需要的计算成本更大,即功率消耗高。而在验证阶段中,可以看出 UAPL 协议消耗在哈希函数上的计算时间相比 Khan-Alghathbar 协议^[11]和 Chen-Shih 协议^[13]都要多,但时间差距较小,由于哈希函数的计算时间很少,因此在这个阶段的功率消耗上 UAPL 协议和这两个协议相差很小,而且 UAPL 协议在验证阶段选择的是保密性更高的用户、网关节点、传感器节点三者之间互相验证方式,因此在加密/解密过程中虽然哈希函数的计算需求量更大,但安全性能更强。

表2 协议对比结果

阶段	节点	UAPL 协议	Khan-Alghathbar 协议	Nyang-Lee 协议	Chen-Shih 协议
注册阶段	用户	$1T$	0	0	0
	网关节点	$3T$	$3T$	$3T$	$3T$
	传感器节点	0	0	0	0
登录阶段	用户	$3T$	$4T$	$4T$	$4T$
	网关节点	0	$1T$	0	0
	传感器节点	0	0	0	0
验证阶段	用户	$1T$	0	$1T + 1T_1$	$1T$
	网关节点	$8T$	$6T$	$9T + 1T_2$	$6T$
	传感器节点	$2T$	$2T$	$1T_1 + 1T_2$	$1T$
密码变更阶段	用户	$3T$	$3T$	—	—
	网关节点	0	0	—	—
	传感器节点	0	0	—	—

5 结语

用户认证协议是合法用户在获取无线传感器网络内部数据过程中的一个重要的安全保护机制,本文改进了 Das 协议的登录用户身份验证机制,提出了一种新的无线传感器网络用户认证协议(UAPL),主要通过加强用户端与网关节点、网关节点与传感器节点之间的互相验证,提高用户认证过程的安全性,并添加了密码变更机制。从对比实验中看出,相对其他改进的 Das 协议,UAPL 协议在遭遇伪装攻击、蛮力攻击时有安全性的防护措施,而且 UAPL 协议与其他改进 Das 协议在功率消耗上差距很小,却有更高的安全性能。

参考文献:

- [1] YAN L, PENG D, GAO Y. Analysis and improvement of sensor networks security protocol[J]. Journal on Communications, 2011, 32(5):139~145. (闫丽丽, 彭代渊, 高悦翔. 传感器网络安全协议的分析和改进[J]. 通信学报, 2011, 32(5):139~145.)
- [2] HONG Y, LI P. Information security defense mechanism based on wireless sensor network correlation[J]. Journal of Computer Applications, 2013, 33(2): 423~467. (洪勇, 李平. 基于无线传感器网络相关性的信息安全防御机制[J]. 计算机应用, 2013, 33 (2): 423~467.)
- [3] LIU Y, YANG L, FAN K. Improved dynamic user authentication protocol[J]. Acta Electronica Sinica, 2013, 41(1): 42~46. (刘云, 杨亮, 范科峰. 一种改进的动态用户认证协议[J]. 电子学报, 2013, 41(1): 42~46.)
- [4] HE Y, TIAN S. Block encryption algorithm based on chaotic S-box for wireless sensor network[J]. Journal of Computer Applications, 2013, 33(4): 1081~1084. (何远, 田四梅. 基于混沌 S 盒的无线传感器网络分组加密算法[J]. 计算机应用, 2013, 33(4): 1081~1084.)
- [5] DAS M L. Efficient user authentication and secure data transmission in wireless sensor networks[C]// Proceedings of the 16th IEEE International Conference on Networks. Piscataway: IEEE, 2008: 1~6.
- [6] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks[J]. ETRI Journal, 2010, 32(5): 704~712.
- [7] 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.

(下转第 476 页)

性。

3.2 系统性能测试

TIFC 在模拟器上运行测试 (Ubuntu 10.04, Android 4.1.1), 由于模拟器与真机实验条件差异, 并不能提供真实的地理位置信息、短信、蓝牙和网络等环境, 同时模拟器较真机效率较低。但模拟器可以通过 DDMS (Dalvik Debug Monitor Service) 提供更加充分的调试命令和虚拟出必要的测试环境。TIFC 对系统性能主要表现在系统调用时间上。通过 logcat 分析系统调用完成时间差, 并与原系统进行对比, 结果如表 2 所示。

表 2 系统调用完成时间差对比

系统调用 API	完成时间差/ms		延迟率/%
	原系统	TIFC 系统	
获取地理位置	62	69	11.2
发送短信信息	72	86	19.4
拍摄图片	555	621	12.4

4 结语

随着移动互联网络的发展, 更多更强大的功能将出现在移动终端上, 甚至, 政府、军队、企业的业务都向移动终端上拓展。安卓作为当前最流行的移动终端平台, 针对其安全研究将会是一项长期而艰巨的任务。

本文针对现有的访问控制模型在保护移动平台数据安全都有一定局限性。借鉴了软件测试中的用于跟踪和分析输入数据在程序内部流向的污点传播机制, 并从吸取传统访问控制模型中的思想, 提出一个基于污点的访问控制模型。TBAC 相比现有访问控制模型更加可用、灵活与细粒度。TBAC 试图通过污点传播分析来解决程序执行过程中产生隐蔽通道问题, 还设计了一个基于污点标记与跟踪的隐私信息控制框架。TIFC 通过分析安卓平台上所有污染源与污染离开点、研究污点在程序执行中的传播方式与途径、控制关键点的信息流向, 能细粒度地、灵活地、准确地实时跟踪应用程序所使用隐私信息并控制隐私信息的流向。下一步将对该模型进行扩展, 以满足不同安全需求, 并对模型进行形式化验证。

参考文献:

- [1] ZHOU Y, JIANG X. Dissecting Android malware: characterization and evolution [C]// IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2012: 95–109.
- [2] LA POLLÀ M, MARTINELLI F, SGANDURRA D. A survey on security for mobile devices [J]. IEEE Communications Surveys & Tutorials, 2012, 15(1): 446–471.
- [3] VIDAS T, VOTIPKA D, CHRISTIN N. All your droid are belong to us: a survey of current Android attacks [C]// Proceedings of the 5th USENIX Conference on Offensive Technologies. Berkeley: USENIX Association, 2011: 10–19.
- [4] MARFORIO C, FRANCILLON A, CAPKUN S, et al. Application collusion attack on the permission-based security model and its implications for modern smartphone systems [R]. Zürich: Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.
- [5] ENCK W, OCTEAU D, MCDANIEL P, et al. A study of Android application security [C]// Proceedings of the 20th USENIX Security Symposium. Berkeley: USENIX Association, 2011: 101–113.
- [6] SMALLEY S, CRAIG R. Security Enhanced (SE) Android: bring flexible MAC to Android [C]// Proceedings of the 2013 Network & Distributed System Security. San Diego: Internet Society, 2013: 75–84.
- [7] ENCK W, ONGTANG M, MCDANIEL P. On lightweight mobile phone application certification [C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009: 235–245.
- [8] NAUMAN M, KHAN S, ZHANG X. Apex: extending Android permission model and enforcement with user-defined runtime constraints [C]// Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2010: 328–332.
- [9] DIETZ M, SHEKHAR S, PISETSKY Y, et al. Quire: lightweight provenance for smart phone operating systems [C]// Proceedings of the 20th USENIX Security Symposium. Berkeley: USENIX Association, 2011: 371–387.
- [10] ENCK W, GILBERT P, CHUN B G, et al. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones [C]// Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2010: 1–6.
- [11] YANG Z, YIN L, DUAN M, et al. Generalized taint propagation model for access control in operation systems [J]. Journal of Software, 2012, 23(6): 1602–1619. (杨智, 殷丽华, 段沫毅, 等. 基于广义污点传播模型的操作系统访问控制 [J]. 软件学报, 2012, 23(6): 1602–1619.)
- [12] LI F H, SU M, SHI G Z, et al. Research status and development trends of access control mode [J]. Journal of Electronics, 2012, 40(4): 805–813. (李凤华, 苏铤, 史国振, 等. 访问控制模型研究进展及发展趋势 [J]. 电子学报, 2012, 40(4): 805–813.)

(上接第 455 页)

- [8] HE W, LIU X, NGUYEN H, et al. PDA: Privacy-preserving data aggregation in wireless sensor networks [C]// Proceedings of the 26th IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE, 2007, 2045–2053.
- [9] DAS M L. Two-factor user authentication in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086–1090.
- [10] TIWARI H, ASAWA K. A secure and efficient cryptographic hash function based on NewFORK-256 [J]. Egyptian Informatics Journal, 2012, 13(3): 199–208.
- [11] 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.
- [12] DYANG D H, LEE M K. Improvement of Das's two-factor authentication protocol in wireless sensor networks [J/OL]. (2009-12-20) [2013-06-20]. <http://eprint.iacr.org/2009/631.pdf>.
- [13] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks [J]. ETRI Journal, 2010, 32(5): 704–712.