第 29 卷第 1 期　　四川理工学院学报(自然科学版)　　Vol. 29　No. 1
2016 年 2 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Feb. 2016
文章编号:1673-1549(2016)01-0033-06　　DOI:10.11863/j.suse.2016.01.08

无线网络认证密钥交换协议 L－MAKEP 的改进

陈泗盛, 蓝红秀, 孙树亮

(福建师范大学福清分校电子与信息工程学院, 福建　福清　350300)

摘　要:L－MAKEP 协议是一种适用于非对等的无线网络的高效的密钥交换协议,该协议具有执行简单且计算复杂度低的优点。分析对比三种攻击方法,表明协议不能抵抗伪造和欺骗攻击,并指出安全问题在于其中的异或运算和公钥身份信息性验证的缺失。因此,在 Yang－Chen 方案的基础上采用身份密码系统,以身份信息作为用户的公钥,并在等式验证公式中引入公钥身份信息,从而实现双方的身份信息验证。同时增加了哈希确认来对弱客户端进行确认。协议的分析表明,改进协议能够正确执行,同时其安全性得到提高。

关键词:无线网络认证;密钥交换协议;L－MAKEP 协议;协议改进
中图分类号:TP393　　**文献标志码**:A

引　言

无线网络是利用无线电射频或红外线等无线传输媒体与技术构成的通信网络系统。无线网络是无线设备之间以及无线设备与有线网络之间的一种网络结构。随着无线网络技术及其应用的迅速发展,网络安全问题成为制约其发展的一个主要因素。

无线设备在存储能力、计算能力、带宽和电源供电等方面具有一定的有限性。因此,无法将在有线网络的安全策略照搬到无线网络中,这就要求设计一些满足无线网络应用环境的安全机制[1-2]。

无线网络的安全数据发送协议和无线网络的密钥管理技术,是当前无线网络研究的一个热点。学者从不同的角度来研究无线网络中的身份认证密钥交换问题,如匿名性[3]、应用环境[4]等。L－MAKEP(Linear－MAKEP)协议[5]是针对非对称式无线网络设计的密钥交换协议,协议的一方可以是计算能力较低的一般节点,另一方要求具有较高的计算能力。该协议由于具有执行简单且计算复杂低的特点而受到很多的跟进研究,例如文献[6－9]从不通的角度对方案进行安全性分析,指出协议的安全问题,并给出相应的攻击方法,文献[10－12]将该协议延伸到 IPTV 和无线射频卡的用户认证中。本文在安全性方面,对比 Shim 方案[6]、Yang－Chen 方案[7]、Liu－Chen 方案[8],进一步分析其安全问题,并在此基础上提出一个能够抵抗这三类攻击的改进方案,并对该方案进行安全性分析。

1　L－MAKEP 认证密钥交换协议

文献[5]提出了一个应用于无线网络的认证密钥交换协议,该协议客户端通过简单的算法处理就可以和服务端进行密钥协商,而且该协议是双向认证协议,所以客户端和服务器都无法欺骗对方。假设 p 是一个素数,

收稿日期:2015-12-01
基金项目:福建省教育厅科技项目(JB14132);福建师范大学福清分校科研创新基金项目(KY2014022)
作者简介:陈泗盛(1981-),男,福建泉州人,讲师,硕士,主要从事网络与信息安全方面的研究,(E-mail)chssh1982@sohu.com;
孙树亮(1982-),男,安徽蚌埠人,副教授,博士,主要从事信息隐藏方面的研究,(E-mail)thussl_07@126.com

满足在 z_p 上求离散对数问题在计算上是不可行的，$g \in z_p$ 是 z_p^* 的一个本原元。用户 A 选取随机整数序列 $(a_1, a_2, \cdots, a_{2m})$ 作为私钥序列，并计算私钥序列对应的公钥序列 $(g^{a_1}, g^{a_2}, \cdots, g^{a_{2m}})$。相邻的两个公钥 $(g^{a_{2i-1}}, g^{a_{2i}})$ 构成一组，并从可信中心 TA 获取相应的公钥证书 $Cert_A^i = < ID_A, g^{a_{2i-1}}, g^{a_{2i}}, Sign_{TA}(ID_A, g^{a_{2i-1}}, g^{a_{2i}}) >$，$1 \leqslant i \leqslant m$。用户 B 公开公钥信息 PK_B，保密私钥 SK_B。协议流程如图 1 所示。

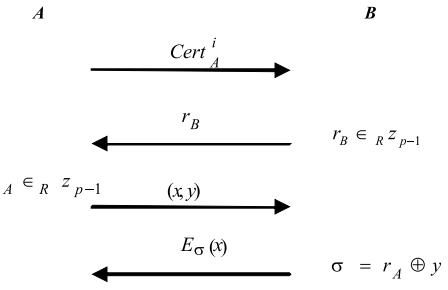

图 1 L – MAKEP 认证密钥交换协议

具体在第 i 轮的协议中，A 和 B 协商认证密钥的过程如下：

(1)用户 A 向用 B 发送证书。证书信息如下：

$Cert_A^i = < ID_A, g^{a_{2i-1}}, g^{a_{2i}}, Sign_{TA}(ID_A, g^{a_{2i-1}}, g^{a_{2i}}) >$

(2)用户 B 首先验证证书的有效性。如验证通过，则选取一个随机数 $r_B \in z_{p-1}$，将其发送给 A。

(3) A 收到随机数 r_B 后，选取另外一个随机数 r_A，并计算：

$$\begin{cases} x = E_{PK_B}(r_A) \\ y \equiv a_{2i-1}(x \oplus r_B) + a_{2i} (\mathrm{mod} p - 1) \\ \sigma = r_A \oplus y \end{cases} \tag{1}$$

将 (x, y) 发送给 B。

(4) B 收到消息 (x, y) 后，验证等式(2)是否成立。

$$(g^{a_{2i-1}})^{x \oplus r_B} g^{a_{2i}} \overset{?}{\equiv} g^y (\mathrm{mod} p) \tag{2}$$

如果等式成立，B 解密 $x = E_{PK_B}(r_A)$ 获取 r_A 并计算 $\sigma = r_A \oplus y$，用 σ 加密消息 x 获得密文 $E_\sigma(x)$，并将其发送给 A。

(5) A 收到消息后，用自己先前计算的 σ 解密密文 $E_\sigma(x)$，如果获取的明文和自己发送的消息 x 一致，则其确认 B 已经获取正确的会话密钥 σ。

协议执行完毕后，A 和 B 都相信它们和另一方面协商出了一个共享密钥 σ。显然在密钥协商的过程中，A 和 B 之间也进行了相互的身份认证。

2 L – MAKEP 方案的安全分析

2.1 Shim 的攻击方法

Shim[6] 针对 L – MAKEP 提出了一种中间人攻击方案，即攻击者 E 实现让用户 B 相消息来源于 E，同时 A 确信自己是与 B 进行通信(图 2)。具体的攻击方法如下：

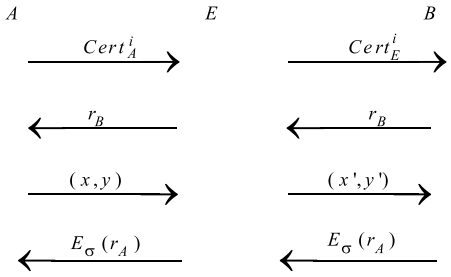

图 2 Shim 攻击方法

(1)攻击者 E 选取随机数 $c \in z_{p-1}$，根据用户 A 的公钥 $(g^{a_1}, g^{a_2}, \cdots, g^{a_{2m}})$ 计算获取公钥序列 $((g^{a_1})^c, (g^{a_2})^c, \cdots, (g^{a_{2m}})^c)$，将此序列作为自己的公钥序列，并向 TA 申请公钥证书。在第 i 轮 E 获取公钥证书：$Cert_E^i = < ID_E, (g^{a_{2i-1}})^c, (g^{a_{2i}})^c, Sign_{TA}(M) >$，其中，$M = ID_E \| (g^{a_{2i-1}})^c \| (g^{a_{2i}})^c$，这里 E 只知道 c，它不知道公钥所对应的私钥 $a_1 c, a_2 c, \cdots, a_{2m} c$。

(2) A 初始化 L – MAKEP 协议，发送 $Cert_A^i$ 给 B。

(3) E 截取 $Cert_A^i$，并用证书 $Cert_E^i$ 替换发送给 B。

(4) B 接收 $Cert_E^i$，确认当前执行协议的是 E。则，B 选取随机数 $r_B \in z_{p-1}$ 发送给 E。

(5) E 将收到的 r_B 转发给 A。

(6) A 接收随机数 r_B，选取另一个随机数 r_A，计算：

$$\begin{cases} x = E_{PK_B}(r_A) \\ y \equiv a_{2i-1}(x \oplus r_B) + a_{2i} (\mathrm{mod} p - 1) \\ \sigma = r_A \oplus y \end{cases} \tag{3}$$

发送 (x, y) 给 B。

(7) E 截取消息 (x, y)，将消息替换成 (x, y')，其中 $y' = yc$，并发送给 B；

(8)当 B 收到消息 (x, y')，验证等式

$$(g^{ca_{2i-1}})^{x \oplus r_B} g^{ca_{2i}} \overset{?}{\equiv} g^{y'} (\mathrm{mod} p) \tag{4}$$

是否成立。因为 $y = ca_{2i-1}(x \oplus r_B) + ca_{2i}$，所以等式(4)成立。$B$ 解密 x 获取明文 r_A，计算会话密钥 $\sigma = r_A \oplus y'$。

将密文 $E_\sigma(x)$ 发送给 E,再由 E 转发给 A。

(9) A 收到消息 $E_\sigma(x)$ 后解密密文,判断明文是否与之前发送的 x 一致,从而确定共享会话密钥 σ 的正确性。

Shim 认为协议执行结束后,A 相信自己和 B 共享了会话密钥 σ,但是 B 认为自己和 E 共享了会话密钥 σ。其实,认真分析 Shim 攻击方法不难发现,步骤(8)中用户 B 计算的会话密钥 $\sigma = r_A \oplus y'$ 和 A 计算的会话密钥 $\sigma = r_A \oplus y$ 是不一致的,因此在步骤(9)中用户 A 收到密文 $E_\sigma(x)$ 后解密出来的明文验证是不能通过的。所以,Shim 攻击不能达到预期的效果。

2.2　Yang－Chen 的攻击方法

Yang－Chen[7] 的攻击方法是基于这样的定理结论:对任意的第 i 轮线性 MAKEP 协议存在多对的 (x, r_B, y) 满足式(2)。定理的证明可以参阅文献[7]。

假设攻击 E 者监听了 A 和 B 的交换过程并记录了交换信息,则 E 可以通过以下方法向 B 发起认证和密钥协商:

(1) E 重放 A 在第 i 轮发送的 $Cert_A^i$ 给 B。

(2) B 验证完 $Cert_A^i$ 的有效性,选取一个随机数 r_B' 发送给 E。

(3) E 接收到 r_B' 后,选取 x', y',满足 $x \oplus r_B = x' \oplus r_B', y = y'$,并发送 (x', y') 给 B。

(4) B 收到消息 (x', y') 后,因为等式(2)能通过验证,所以其相信 E 是合法的用户。

Yang－Chen 同时也给出针对上述攻击方法的改进方法:

(1)在式(1)中 y 的计算用以下式子替代:

$$y \equiv a_{2i-1} r_B + a_{2i} x (\mathrm{mod} p - 1) \tag{5}$$

(2) 式(2)的验证等式改为:

$$(g^{a_{2i-1}})^{r_B} (g^{a_{2i}})^x \overset{?}{\equiv} g^y (\mathrm{mod} p) \tag{6}$$

新的 y 的计算已经取消了异或运算,因此 Yang－Chen 的攻击方法已经失效,因此想伪造 x', y' 使得等式 $(g^{a_{2i-1}})^{r_B} (g^{a_{2i}})^x \equiv g^y (\mathrm{mod} p)$ 成立需要进一步的研究与分析。

2.3　Liu－Chen 的攻击方法

文献[8]中提出了一种类似于 Yang－Chen 的攻击方法,这里称之为 Liu－Chen 攻击法,它也是针对协议的异或运算提出了伪造方案。Yang－Chen 的攻击方法中只说明了存在 x', y' 满足 $x \oplus r_B = x' \oplus r_B'$,具体的 x', y' 如何选取没有给出方法,Liu－Chen 方案给出了具体的 x', y' 的构造方法。该攻击方法是基于以下结论:

(1) 如果 a, b 是两个奇数,则有:

$$a \oplus b = (-a) \oplus (-b)$$

(2) 如果 a, b 是偶数,且 $4 \mid a, b$,同时 $8 \nmid a, b$,则有:

$$a \oplus b = (-a) \oplus (-b)$$

假设攻击 E 者监听了 A 和 B 的交换过程并记录了交换信息,则 E 可以通过图 3 所示的方法向 B 发起认证和密钥协商。

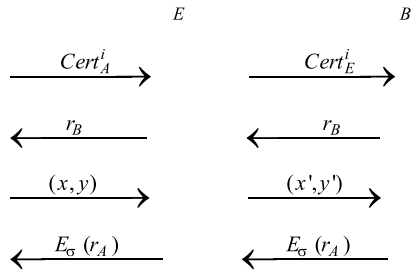

图 3　Liu－Chen 攻击方法

(1) E 重放 A 在第 i 轮发送的 $Cert_A^i$ 给 B。

(2)当 B 验证完 $Cert_A^i$ 的有效性后,选取一个随机数 r_B' 发送给 E。

(3) E 接收到 r_B' 后,计算 $x' \equiv -x(\mathrm{mod} p - 1)$, $r'_B \equiv -r_B(\mathrm{mod} p - 1)$,则满足:

$$(x', y'): x \oplus r_B = x' \oplus r_B', y' = y \tag{7}$$

并将 (x', y') 发送给 B。

(4) B 收到消息 (x', y') 后,能正确验证式(2),所以其相信 E 是合法的用户。

3　L－MAKEP 认证密钥交换协议的改进

分析可知:一方面,虽然 Shim 攻击并不能达到预期的目的,但是从其攻击方法分析中不难发现,由于在执行过程中缺少对 A 的公钥的验证,而且在发送消息过程中没有体现身份信息,因此协议对这类中间人攻击和重放攻击是存在安全风险的,这一点在文献[9]中也有提到;另一方面,Yang－Chen 和 Liu－Chen 的攻击都是针对协议中的异或运算的特点提出的,虽然 Yang－Chen 针对这类攻击提出了改进的方法,但是其并没有解决中间人攻击与重放攻击这一类安全问题。本文在 Yang－

Chen 提出的改进方法的基础上,对前述安全问题进行进一步解决。

3.1 改进的 L – MAKEP 密钥交换协议

为了解决身份欺骗问题,在 Yang – Chen 方案的基础上采用基于身份的密码算法。用户的公钥是用户的身份信息 ID,如 A 的公钥是 ID_A,由可信中心 TA 为用户计算私钥,如公钥 ID_A 对应的私钥是 s_A。获取公钥对应的私钥后,在协议中产生的公钥序列就不需要从证书中心获取证书序列了,用户自己可以用自己的私钥计算出其他用户可以利用公共参数验证的公钥序列。具体的方案如图 4 所示。

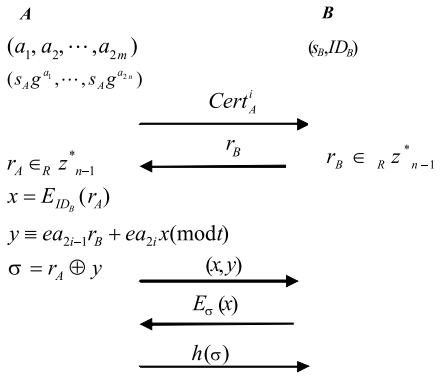

图 4 改进 L – MAKEP 密钥交换协议

3.1.1 用户注册

可信中心 TA 选择两个大素数 p,q,计算 $n = pq$,TA 再选取算法参数 e,d,满足 $ed \equiv 1(\mathrm{mod}\ \varphi(n))$,以及与 p,q 都互素的数 g,并保证 g 有较高的阶,且其阶为 t。TA 公开 n,e,g,t,其他参数保密。

任何用户在使用密钥协商之前需要向 TA 注册,从而获得身份的私钥。注册过程如下:

(1)用户 A 将自己的身份信息 ID_A 发送给 TA,这里 ID_A 是模 n 下的一个整数。

(2) TA 计算 A 的私钥 $s_A \equiv (ID_A)^{-d}(\mathrm{mod}\ n)$,并通过安全信道发送给用户 A。

用户 A 公开自己的公钥 ID_A,保密自己的私钥 s_A。

3.1.2 协议的执行

用户 A 随机选取长度为偶数的整数序列 $(a_1, a_2, \cdots, a_{2m})$,其中 $1 \leqslant a_i \leqslant n-1, i = 1,2,\cdots,2m$,作为私钥序列。并计算私钥序列对应的公钥序列 $(s_A g^{a_1}, s_A g^{a_2}, \cdots, s_A g^{a_{2m}})$。

则在第 i 轮的协议中 A 和 B 协商认证密钥的过程如下:

(1)用户 A 将 $Cert_A^i = < ID_A, s_A g^{a_{2i-1}}, s_A g^{a_{2i}} >$ 发送给用户 B。

(2) B 选取一个随机数 $1 \leqslant r_B \leqslant n-1$,将其发送给 A。

(3) A 收到随机数 r_B 后,选取另外一个随机数 $1 \leqslant r_A \leqslant n-1$,并计算:

$$x = E_{ID_B}(r_A)$$
$$y \equiv ea_{2i-1} r_B + exa_{2i} (\mathrm{mod}\ t) \tag{8}$$
$$\sigma = r_A \oplus y$$

将 (x,y) 发送给 B。

(4)B 收到消息 (x,y) 后,验证等式

$$(s_A g^{a_{2i-1}})^{er_B} (ID_A)^{r_B} (s_A g^{a_{2i}})^{ex} \overset{?}{\equiv} (ID_A)^{-x} g^y (\mathrm{mod}\ n)$$

如果等式成立,B 解密 $x = E_{PK_B}(r_A)$ 获取 r_A 并计算 $\sigma = r_A \oplus y$,用 σ 加密消息 x 获得密文 $E_\sigma(x)$,并将其发送给 A。

(5) A 收到消息后,用自己先前计算的 σ 解密密文 $E_\sigma(x)$,如果获取的明文和自己发送的消息 x 一致,则其确认 B 已经获取正确的会话密钥 σ。A 回复消息 $h(\sigma)$ 给 B。

(6) B 收到确认消息 $h(\sigma)$ 后,可以确认已经获取正确的会话密钥。

3.2 改进协议的分析

3.2.1 正确性分析

正确的 (x,y) 是能够通过 $(s_A g^{a_{2i-1}})^{er_B} (ID_A)^{r_B} (s_A g^{a_{2i}})^{ex} \overset{?}{\equiv} (ID_A)^{-x} g^y (\mathrm{mod}\ n)$ 验证。

证明 因为,$s_A \equiv (ID_A)^{-d}(\mathrm{mod}\ n)$,$y \equiv ea_{2i-1} r_B + exa_{2i}(\mathrm{mod}\ t)$ 所以,

$$\begin{aligned}
&(s_A g^{a_{2i-1}})^{er_B} (ID_A)^{r_B} (s_A g^{a_{2i}})^{ex} \\
&= (s_A g^{a_{2i-1}})^{er_B} (ID_A)^{r_B} (s_A g^{a_{2i}})^{ex} \\
&\equiv (ID_A)^{-edr_B} \cdot g^{ea_{2i-1} r_B} \cdot (ID_A)^{r_B} \cdot (ID_A)^{-edx} g^{ea^*_{2i}} \\
&\equiv (ID_A)^{-x} g^{ea_{2i-1} r_B + ea_{2i} x^*} \\
&\equiv (ID_A)^{-x} g^y (\mathrm{mod}\ n)
\end{aligned}$$

3.2.2 安全性分析

(1)在改进方案中,已经取消了异或的运算,其中 $y \equiv ea_{2i-1} r_B + exa_{2i}(\mathrm{mod}\ t)$,所以针对异或运算的 Yang

– Chen 和 Liu – Chen 攻击已经无效。

(2)在验证等式:$(s_A g^{a_{2i-1}})^{er_B}(ID_A)^{r_B}(s_A g^{a_{2i}})^{-ex} \overset{?}{\equiv} ID_A g^{y} (\mathrm{mod}\ n)$ 中,包含了用户 A 的身份信息,因此当 E 想假冒 A 向 B 发起协商,由于 E 不知道 ID_A 对应的私钥 s_A,因此无法构造出与 ID_A 对应的 (x,y) 来通过验证的,即对消息的真实性进行了认证。因此,像 Shim 之类的中间攻击也已经不能奏效。

3.2.3　性能分析

改进的认证方案与 L – MAKEP 两个协议在执行方式上主要存在三方面不同。

(1)用户 A 的公钥证书获取。原方案是对每组公钥 $(g^{a_{2i-1}}, g^{a_{2i}})$ 都从中心获取证书,改进方案公钥证书是由用户的私钥计算得到。在这方面,原方案有通信消耗,而改进方案不需要进行通信但有计算消耗。

(2)用户 A 计算 (x,y)。L – MAKEP 协议和改进协议都包含一个加密运算、一个模下的乘法运算和一个异或运算。不同的是,在模下的乘法运算中,改进协议用数乘运算代替了异或运算,这一计算量的增加相对于模下的指数运算是不明显的。

(3)用户 B 的等式验证。改进方案验证等式:

$$(s_A g^{a_{2i-1}})^{er_B}(ID_A)^{r_B}(s_A g^{a_{2i}})^{ex} \overset{?}{\equiv} (ID_A)^{-x} g^{y} (\mathrm{mod}\ n)$$

较 L – MAKEP 方案的等式

$$(g^{a_{2i-1}})^{x \oplus r_B} g^{a_{2i}} \overset{?}{\equiv} g^{y} (\mathrm{mod}\ p)$$

多了身份方面的计算。

综上,改进协议整体计算量的增加主要体现在用户 B 验证等式。但是协议适用的不对等无效网络,即用户 B 比用户 A 具有更多的计算资源,因此可以认为改进方案是有效的。

4　结束语

密钥交换协议是无线网络安全中的一个重要的研究问题,是无线网络中密钥管理技术的一个重要组成部分。本文对比分析了 Shim 攻击、Yang – Chen 攻击和 Liu – Chen 攻击,指出 L – MAKEP 不能抵抗中间人攻击的弱点。在 Yang – Chen 的改进方法的基础上引进了用户双方的身份信息,并以此作为公钥,应用身份密码算法实现身份认证,并通过最后的共享密钥的确认来对弱客户端进行认证。最后,对改进的协议进行了正确性、安全性和性能的分析,通过分析表明改进协议具有合理性和有效性。

参 考 文 献:

[1] 冯登国.安全协议-理论与实践[M].北京:清华大学出版社,2011:273-316.

[2] 朱建明,马建峰.无线局域网安全:方法与技术[M].北京:机械工业出版,2005:2-15.

[3] LEE C C,LI C T,HSU C W.A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps[J]. Nonlinear Dynamics,2013,73(1):125-132.

[4] DAVID D B,RAJAPPA M,KARUPUSWAMY T,et al. Secure mutual authentication and Key-Agreement protocol for IP Multimedia Server-Client[J]. Journal of Computational & Theoretical Nanoscience,2014,20(11):1856-1863.

[5] WONG D S,CHAN A H.Mutual authentication and key exchange for low power wireless communications[C]// Proceeding of Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force, IEEE,Boston,USA,October 28-31,2001(1):39-43.

[6] SHIM K.Cryptanalysis of mutual authentication and key exchange for low power wireless communications[J]. IEEE Communications Letters,2003,7(5):248-250.

[7] YANG F Y,CHEN R C.On the security of mutual authentication and key exchange for low power wireless communications[J].Chien-Kuo Journal,2003,22:611-615.

[8] LIU C L,CHEN S S,SUN S L. Security analysis of mutual authentication and key exchange for low power wireless communications[J]. Energy Procedia,2012,17:644-649.

[9] SIAW L N,CHRIS M.Comments on mutual authentication and key exchange protocols for low power wireless communications[J].IEEE communications letters,2004,8(4):262-263.

[10] LEE C C,LI C T,CHEN C T,et al. A new key

exchange protocol with anonymity between STB and Smart Card in IPTV Broadcasting[C]//Proceeding of 7th International Conference on Wireless communications,Networking and Mobile Computing,IEEE,Wuhan,China,September 23-25,2011:1-4.

[11] JUN E A,RHEE H S,JIM J G,et al.Fingerprint-based access control using smart cards in IPTV[J].Multimedia Tools and Applications,2014,73(2):647-661.

[12] LEE C C,CHEN C T, LI C T,et al.A practical RFID authentication mechanism for digital television[J].Telecommunication Systems,2014,57(3):239-246.

Improvement of Linear Mutual Authentication and Key Exchange Protocol for Wireless Network

CHEN Sisheng, *LAN Hongxiu*, *SUN Shuliang*

(School of Electronic and Information Engineering, Fuqing Branch of Fujian Normal University, Fuqing 350300, China)

Abstract: L-MAKEP Protocol is an efficient key exchange protocol that is suitable for the equivalence wireless network, which has the advantages of simple implementation and low computational complexity. Analysis and comparison of three kinds of attacks indicates that the protocol doesn't overcome the forgery and spoofing attacks, and it is pointed out that security problem is to lack of XOR operation and doesn't verifying the public key. The refore, an improved Key Exchange Protocol which cancels the XOR operation and applies the identity information based on the Yang-Chen program was put forward. At the same time it increase the hash to confirm the weak client to confirm. The analysis of the protocol indicated that the improved protocol can be executed correctly and more security.

Key words: identity authentication; wireless network; key exchange protocol; linear-MAKEP; improved protocol