一种新颖的基于Hash函数的无线双向安全认证方案

王杰华 刘会平 邵浩然 夏海燕
(南通大学计算机科学与技术学院 南通 226019)

摘 要 随着科技的不断发展,越来越多的网络设备接入到无线网络中,为了确保合法用户的正确识别连接,在Wen-Li认证方案的基础上提出了一种基于Hash函数的无线双向安全认证方案。该方案通过引入发送包序列号代替时间戳,避免网络延时对认证过程产生影响,且不需要设备之间时钟的严格同步。安全性与运算量的对比分析表明,较Wen-Li方案,所提方案能有效避免各种常见的网络攻击,具有更高的安全性,且运算量较小,计算复杂度较低,能有效降低实际系统的开销。

关键词 双向认证,Hash函数,包序列号,中间人攻击,离线口令猜测攻击
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.040

Novel Two-way Security Authentication Wireless Scheme Based on Hash Function

WANG Jie-hua LIU Hui-ping SHAO Hao-ran XIA Hai-yan
(School of Computer Science and Technology, Nantong University, Nantong 226019, China)

Abstract With the development of science and technology, more and more network devices are connected to the wireless network. In order to ensure the legitimate users' correct identification and connections, based on the Wen-Li authentication scheme, a novel two-way security authentication wireless scheme based on hash function(TSAWSH) was proposed. By using the send packet sequence number instead of of timestamp, the TSAWSH can avoid the influence to the certification process caused by the network delay and needn't the strict clock synchronization between the devices. By comparing the security and complexity analyses with the Wen-Li scheme, the TSAWSH can effectively avoid the common network attacks, has higher safe property and less computational quantity, and also has lower computational complexity. The TSAWSH can effectively reduce the overhead of the actual system.

Keywords Two-way authentication, Hash function, Packet sequence number, Man-in-the-middle attack, Off-line password guessing attack

1 引言

随着无线网络和移动设备的迅速发展,用户可以在任何时间、任何地点通过移动设备(如智能手机、PDA等)获取网络资源,使人们的生活更加便捷[1]。但是,随着大量的无线设备的接入以及各种恶意攻击的增加,网络信息安全问题已成为基于互联网服务的重要议题,信息的安全传输日益受到人们的重视[2]。确保通信网络和数据安全的首要条件就是在众多网络设备中准确鉴别出用户身份[3]。身份认证是一种与密码学相结合,能准确鉴别用户身份是否合法的技术,目前国内外众多学者对其进行了研究并提出了相关方案。

1981年Lamport[4]首先提出了一种不安全通信中基于用户口令的认证方案,通过构建的密码表验证用户的合法性。然而该方案中Hash运算开销过大,不适于系统的实际应用。2000年Hwang等[5]提出了一种基于智能卡的远程用户认证方案,该方案能有效地避免常见网络攻击,但用户不能自由选择用户口令,面对各种模拟攻击时其安全性也不高[6]。2004年Das等[7]提出了一种基于ID的动态远程用户认证方案,该方案实现简单可靠,具有允许用户自由选择、改变登陆口令、不需要维护任何匹配表等优点。随后,众多学者对Das方案进行了研究并提出了改进方案,2009年Wang等[8]对Das方案进行了分析,同时提出了一种增强型双向认证方案,并证明其具有更高的安全性。2012年,Wen等[9]指出Wang方案存在无法避免伪装攻击及内部攻击等问题,进而提出一种改进方案,解决了Wang方案中存在的安全问题,该方案具有更高的安全性。但2014年,Karuppiah M等[10]指出Wen等提出的方案存在离线口令猜测攻击以及拒绝服务攻击的危险,同时甘宏等[11]也指出Wen方案[9]存在中间人攻击的危险,所以Wen方案并不能满足认证过程对安全的要求。

以上方案均采用时间戳的方式来保证验证消息的新鲜性,即判断 $T'\leqslant T+\Delta T$ 是否成立,其中 ΔT 为网络延时。若消息的接收时间大于发送时间与网络延时的和,则判定该消息无效。这种方法要求网络终端与服务器的时间严格同步,但是随着目前网络设备的不断发展,越来越多的网络终端加入到移动网络中,使得所有终端与服务器时间的严格同步变得异常困难,很多学者针对该问题进行了研究并提出了相应

到稿日期:2015-09-02 返修日期:2016-01-27 本文受国家自然科学基金面上项目(61170171),江苏省"六大人才高峰"项目(2010-WLW-006),江苏省高校科研成果产业化推进项目(JHB2011-45),南通大学研究生创新项目(YKC14018)资助。
王杰华(1965-),男,硕士,副教授,主要研究方向为网络安全、数字水印,E-mail:wang.jh@ntu.edu.cn;刘会平(1990-),男,硕士生,主要研究方向为信息安全;邵浩然(1975-),男,硕士,副教授,主要研究方向为数据挖掘、机器学习;夏海燕(1991-),女,硕士生,主要研究方向为信息安全。

的认证方案。其中，邱慧敏等[3]提出利用计数器和随机数代替时间戳来完成用户与服务器双向认证的方案。但它需要同时使用计数器和随机数发生器，对实际系统造成很大开销。2008 年 Liu 等[12]提出一种利用随机数来完成双向认证的方案。2010 年 Huang 等[13]指出 Wen 方案无法避免伪造攻击并提出了相应的增强方案，但该方案需要利用一个关键信息中心(Key Information Center，KIC)来产生两个大素数以进行相应计算，系统运行复杂且计算量较大。

基于以上分析，本文提出一种新颖的基于 Hash 函数的无线双向认证方案，由于 Hash 函数具有单向性、弱碰撞性和强碰撞性 3 种性质，其具有较高的安全性，常用来产生唯一的认证指纹以进行用户端和服务器端的认证。同时本文利用发送包序列号 PN 不断更新的特性来验证消息新鲜性，可靠地实现了用户与服务器的相互认证。

2 Wen-Li 方案

2.1 Wen-Li 方案回顾

2012 年，Wen 等[9]提出了一种基于 ID 的动态认证方案，它包括两个基本方案：双向认证方案以及密钥协商方案，双向认证方案的实现过程主要由以下 3 个部分组成：注册阶段、登录阶段和认证阶段。本文将对该双向认证方案进行分析与改进，表 1 列出了 Wen-Li 双向认证方案中所用符号的含义。

表 1 符号含义

符号	含义
U_i	用户 i
S	远程服务器
M	恶意用户
CIDi	用户 i 动态身份标识
x	服务器端密钥
ID_i	用户 i 身份标识
PW_i	用户 i 登录口令
T	时间戳
h(.)	单向 Hash 函数
‖	数据连接
⊕	异或运算
A→B	A 通过公共信道向 B 传输信息
A⇒B	A 通过安全信道向 B 传输信息

Wen-Li 双向认证方案的具体实现过程如图 1 所示。

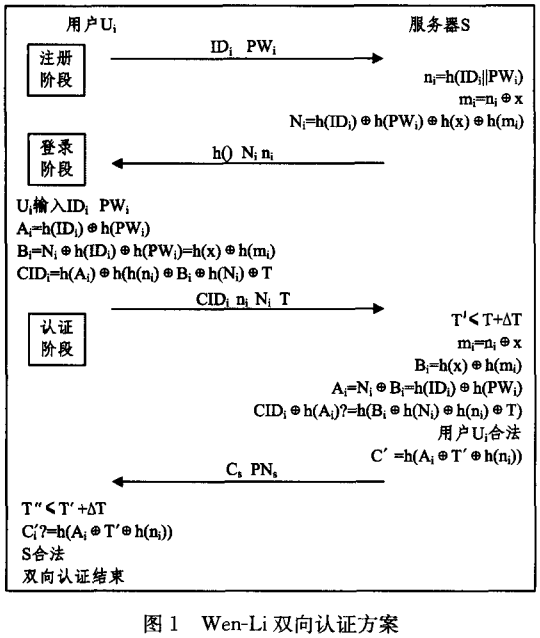

图 1 Wen-Li 双向认证方案

2.1.1 注册阶段

使用该方案时，首先用户 U_i 需向远程服务器 S 进行注册，具体执行步骤如下：

(1)用户 U_i 随机选择 ID_i 和 PW_i，并将 ID_i 和 PW_i 通过安全信道发送给 S 进行注册；

(2)S 获得 U_i 的 ID_i 和 PW_i 后，根据协议的公式计算出 n_i，m_i 以及 N_i 的值，其中 n_i 是 S 持有关于 U_i 信息的唯一值，以通过 n_i 判断智能卡的合法性；

(3)S 将信息 N_i，n_i 以及 Hash 函数存储在智能卡中并通过安全信道发送给 U_i。

该注册步骤仅当新用户加入网络时执行，且对于一个用户只执行一次。

2.1.2 登录阶段

当 U_i 向 S 提交登录请求时，U_i 向智能卡输入 ID_i 和 PW_i，随后智能卡将执行以下操作：

(1)U_i 根据协议规定的公式计算出 A_i，B_i 以及 CID_i 的值；

(2)U_i 通过公共信道将计算出的 $\{CID_i, n_i, N_i, T\}$ 打包发送给 S 进行验证。

2.1.3 认证阶段

当 S 在 T' 时接收到 U_i 的认证申请信息后，执行以下操作：

(1)检查时间戳的有效性，即检查 $T' \leqslant T+\Delta T$ 是否成立；同时判断 n_i 是否在注册列表中。若同时满足两条件，则 S 执行步骤(2)，否则退出认证；

(2)S 根据协议公式以及 S 的私有密钥 x 计算出 m_i，A_i 和 B_i 的值；

(3)S 利用步骤(2)中的 A_i 进行 Hash 运算获得 $h(A_i)$，将 $h(A_i)$ 与 U_i 发送的 CID_i 进行异或运算，并判断所得结果是否与 S 利用 $h(B_i \oplus h(N_i) \oplus h(n_i) \oplus T)$ 重新计算获得的 Hash 值一致，若一致，则 U_i 认证成功，并计算出 C' 的值；否则认证失败；

(4)S 将 C' 值与系统时间 T' 通过公共信道发送给 U_i；

(5)U_i 在 T'' 时刻接收信息后验证时间戳的有效性，若有效则执行步骤 6，否则退出认证；

(6)U_i 利用登录阶段步骤(1)中计算出的 A_i 和 S 发送的时间 T' 和智能卡中保存的 n_i，同时利用 $h(A_i \oplus T' \oplus h(n_i))$ 计算出相应的 Hash 值，判断该值是否与 U_i 发送的 CID_i 的值相等，若相等，则判定 S 合法，双向认证成功；否则双向认证失败。

完成以上步骤后即完成了 Wen-Li 双向认证方案的全部认证过程。

2.2 Wen-Li 方案性能分析

相比于 Wang 方案，Wen-Li 方案取得了很大的进步，弥补了 Wang 方案的众多缺陷，但该方案仍存在不足之处，不能实现预期的安全目标。本文将对其进行分析。

2.2.1 离线口令猜测攻击

U_i 向 S 发送验证申请信息，信息通过共用信道传送，恶意用户 M 可以获得信息中的 n_i，故 M 可以随机选取一对 $(ID_i^*, PW_i^*) \in D_{id} \times D_{pw}$，$D_{id}$ 和 D_{pw} 分别为 ID 和 PW 的取值空间，使得 $n_i^* = h(ID_i^* \| PW_i^*) = n_i$，从而获得真正的 ID 和 PW。

2.2.2 智能卡丢失攻击

假设用户智能卡丢失或者 M 暂时获得智能卡 U_i 的使用

权限，则 M 可以通过密码变更请求修改用户的 PW，并构建 $N_i^* = N_i \oplus h(PW_i) \oplus h(PW_i^*)$ 更新原有的 N_i，使得合法用户 U_i 使用该智能卡认证时认证失败。

2.2.3 严格时间同步

该方案验证使用时间戳的方式对消息新鲜性进行验证，即满足 $T' \leqslant T + \Delta T$ 时该消息是新鲜的。随着接入网络的移动终端的不断增加，所有移动设备时间严格同步异常困难，而且当网络中出现较大延迟时，即 ΔT 值超出一定范围时，认证过程将会出现差错，合法用户不能正常连接。

通过以上分析，M 可以利用 Wen-Li 方案中的不足完成对用户数据的窃取，给合法用户造成严重的损失，本文在保有 Wen-Li 方案优点的基础上，提出了一种新的双向认证方案。

3 基于 Hash 函数的无线双向安全认证方案

通过对 Wen-Li 方案进行了回顾，分析了 Wen-Li 方案中的不足，针对这些不足提出了一种新的双向认证方案，通过使用发送包序列号的方式代替时间戳的使用，以避免网络延迟对认证过程的影响；同时对 Wen-Li 方案进行改进，改进方案能有效地提高认证系统的安全性和可靠性。如图 2 所示，本文方案主要包括 3 个基本阶段：注册阶段、登录阶段和认证阶段。为了便于对本文方案进行叙述，表 2 列出了本文认证方案中的符号含义。

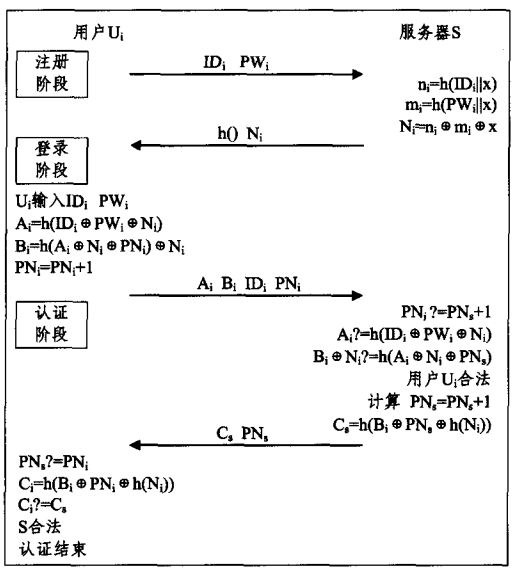

图 2 基于 Hash 函数的无线双向认证方案

表 2 符号含义

符号	含义
U_i	用户 i
S	远程服务器
M	恶意用户
x	服务器端密钥
ID_i	用户 i 身份标识
PW_i	用户 i 登录口令
PN_i	用户移动端保存的最后一次发送包序列号
PN_s	服务器端保存的最后一次发送包序列号
$h(\cdot)$	单向 Hash 函数
$\|$	数据连接
$\oplus$	异或运算
A→B	A 通过公共信道向 B 传输信息
A⇒B	A 通过安全信道向 B 传输信息

3.1 注册阶段

在认证阶段之前，新用户 U_i 必须在服务器端进行注册，具体执行步骤如下：

(1)U_i 选择合适的 ID_i 和 PW_i，并通过安全信道传输给服务器 S。

$U_i \Rightarrow S: \{ID_i, PW_i\}$

(2)服务器 S 计算 n_i，m_i 和 N_i 的值：

$$n_i = h(ID_i \| x) \tag{1}$$

$$m_i = h(PW_i \| x) \tag{2}$$

$$N_i = n_i \oplus m_i \oplus x \tag{3}$$

(3)服务器 S 将 Hash 运算函数以及 N_i 传送给 U_i。

$S \Rightarrow U_i: \{h(\cdot), N_i\}$

3.2 登录阶段

用户 U_i 登录完成验证时，将在用户端执行以下操作：

(1)U_i 输入注册时选定的 ID_i 和 PW_i，并计算 A_i 和 B_i 的值：

$$A_i = h(ID_i \oplus PW_i \oplus N_i) \tag{4}$$

$$B_i = h(A_i \oplus N_i \oplus PN_i) \oplus N_i \tag{5}$$

(2)更新用户端发送的包序列号：

$$PN_i = PN_i + 1 \tag{6}$$

(3)U_i 将 A_i，B_i，ID_i，PN_i 发送给 S：

$U_i \rightarrow S: \{A_i, B_i, ID_i, PN_i\}$

3.3 认证阶段

S 接受 U_i 发送的验证信息后，将对其进行判断并构造服务器端的认证信息完成双向认证，具体步骤如下：

(1)S 收到信息后，判断发送数据包的有效性，即验证等式 $PN_i = PN_s + 1$ 是否成立，若成立，则根据 ID_i 查找本地保存的对应的 PW_i 以及 N_i，并判断以下等式是否成立：

$$A_i = h(ID_i \oplus PW_i \oplus N_i) \tag{7}$$

$$B_i \oplus N_i = h(A_i \oplus N_i \oplus PN_s) \tag{8}$$

若式(7)、式(8)均成立，则用户认证成功，执行步骤(2)；否则退出认证。

(2)更新服务器端发送包序列号：

$$PN_s = PN_s + 1 \tag{9}$$

(3)计算 C_i 的值：

$$C_i = h(B_i \oplus PN_s \oplus h(N_i)) \tag{10}$$

(4)S 将 C_i 和 PN_s 发送给 U_i：

$S \rightarrow U_i: \{C_i, PN_s\}$

(5)U_i 接收信息后判断等式 $PN_i = PN_s$ 是否成立，若成立则执行步骤 6，否则认证失败。

(6)U_i 计算 C_i' 的值：

$$C'_i = h(B_i \oplus PN_i \oplus h(N_i)) \tag{11}$$

判断 C_i' 与 C_i 的值是否相等，若相等，则认证成功，双向认证结束；否则认证失败。

完成以上 3 个基本阶段即可实现本文提出的无线双向认证方案，通过该方案的实现，既可以准确地识别出无线网络中的合法用户，避免恶意用户的非法连接，同时能有效地避免无线网络中常见的网络攻击。

4 性能分析

4.1 安全性分析

本文在 Wen-Li 方案的基础上提出了一种新的双向认证方案，表 3 列举了本文提出的方案与其他方案在安全性方面的比较，其中 O 表示可以防御，×表示不可防御。

表3 安全性对比

	Das方案	Wang方案	Wen-Li方案	本文方案
双向认证	否	是	是	是
重放攻击	O	O	O	O
伪装攻击	×	×	O	O
内部攻击	O	×	O	O
中间人攻击	O	O	×	O
离线口令猜测攻击	×	O	×	O

4.1.1 伪装攻击

本文提出的方案可以有效抵御伪装攻击。在注册阶段，服务器 S 提取本地保存的私有密钥 x 与 U_i 的 ID_i 和 PW_i 值进行运算得到 N_i，N_i 在登录以及认证阶段均不通过明文进行传输，恶意用户 M 并不能通过传输的信息得到 N_i，且该值参与通信双方发送信息的构建，故 M 不能伪装成 U_i 与 S 之间的任意一方，或者截取信息进行篡改后发动伪装攻击。

4.1.2 内部攻击

当该网络中有多台 U_i 进行注册时，由于 x 为服务器 S 的私有密钥，并不会向 U_i 透露私有密钥 x，而是通过公式：$N_i=n_i\oplus m_i\oplus x=h(ID_i\|x)\oplus h(PW_i\|x)\oplus x$ 构建 N_i 验证发送消息的可靠性，假设 M 向服务器进行合法注册获得 N_M，由于 Hash 函数的单向性，M 根据 N_M 推出 x 的值是不可行的，因此即使 M 获得 U_i 的 ID_i 和 PW_i，也不能获得正确的 N_i，故本方案可以有效抵御内部攻击。

4.1.3 离线口令猜测攻击

当 U_i 和 x 相互发送验证信息时，M 可以窃听获得 ID_i，A_i 和 PW_i 等所有信息，但 N_i 并不通过明文在网络上传输，所以 M 不能得到 N_i 的值，从而无法根据 $A_i=h(ID_i\oplus PW_i\oplus N_i)$ 采用离线口令猜测的方式获得 PW_i，故本方案可以有效抵御离线口令猜测攻击。

4.2 运算量分析

表4将 Wang 方案、Wen-Li 方案与本文方案的运算量进行了对比，列举了3种方案在不同阶段中 U_i 与 S 的运算量，其中 t_h 表示一次 Hash 运算的开销，t_x 表示一次异或运算的开销。

表4 运算量对比

	注册阶段		登录阶段		认证阶段		合计
	U_i	S	U_i	S	U_i	S	
Wang方案	0	$2t_h+2t_x$	$2t_h+4t_x$	0	$2t_h+2t_x$	$3t_h+8t_x$	$9t_h+16t_x$
Wen-Li方案	0	$5t_h+4t_x$	$6t_h+6t_x$	0	$2t_h+2t_x$	$7t_h+9t_x$	$20t_h+21t_x$
本文方案	0	$2t_h+2t_x$	$2t_h+5t_x$	0	$2t_h+2t_x$	$4t_h+7t_x$	$10t_h+16t_x$

所提方案中的计算仅使用简单的单向 Hash 运算以及异或运算，不进行指数操作或对称密钥加解密操作，Li 等人[14]指出，通常情况下，运算复杂度可以表示为：$T_E\gg T_H\approx T_S$，其中 T_E，T_H 和 T_S 分别代表指数运算、Hash 运算和对称加解密运算的时间复杂度。相比于指数运算，本文选择的 Hash 运算具有运算简单、系统开销小的特点，同时避免了对称加解密运算中密钥管理复杂的问题。在实际系统的使用过程中，本方案能有效避免因用户移动端数据处理过于复杂给系统带来的压力，降低了移动设备对数据处理性能的要求，有利于本文方案的推广使用。从表4可以看出，本文方案具有更小的运算量，相比于 Wen-Li 方案中使用的 20 次 Hash 运算以及 21 次异或运算，本文方案仅使用了 10 次 Hash 运算以及 16 次异或运算，运算量大幅减小，在实际使用中能有效地降低系统开销。

结束语 本文在对 Wen-Li 方案进行分析后，在其基础上提出了一种新的无线双向安全认证方案。通过安全性分析，本文方案在保留原方案优点的情况下，有效地解决了中间人攻击等常见攻击方式，确保在无线网络中信息传输的安全性和可靠性。通过运算量的对比分析，本方案使用了更少的运算，有效地降低了实际系统的运算开销。同时，本方案验证过程中不使用时间戳，能有效解决网络设备时间同步困难的问题，避免了网络延时对认证过程产生的影响。在接下来的工作中，本文提出的方案将会应用于实际系统，检测在实际使用中本文方案的优越性与可行性，同时加强对认证结束后会话密钥建立阶段的研究与分析。

参考文献

[1] Saraswathi S, Renuka D S, Yogesh P. Secure and efficient Smart-Card-Based remote user authentication scheme for multi-server environment[J]. Candian Journal of Eelectrical and Computer Engineering, 2015, 38(1): 20-30

[2] Chen Yan-li, Du Ying-jie, Yang Geng. Efficient attribute-based authenticated key agreement protocol[J]. Computer Science, 2014, 41(4): 150-154(in Chinese)
陈燕俐，杜英杰，杨庚. 一种高效的基于属性的认证密钥协商协议[J]. 计算机科学，2014，41(4)：150-154

[3] Qiu Hui-ming, Yang Yi-xian, Hu Zheng-min. A new mutual user authentication scheme using smart card[J]. Application Research of Computer, 2005, 22(12): 103-105(in Chinese)
邱慧敏，杨义先，胡正民. 一种新的基于智能卡的双向身份认证方案设计[J]. 计算机应用研究，2005，22(12)：103-105

[4] Lamport L. Password authentication with insecure communication[J]. Communication of the ACM, 1981, 24(11): 770-772

[5] Hwang M S, Li L H. A new remote user authentication scheme using smarts[J]. IEEE Transactions on Consumer Electronics, 2000, 46(1): 28-30

[6] Zhan Li, Yao Guo-xiang, Qiang Heng-chang. Improved mutual authentication scheme based on smartcard for cloud computing [J]. Computer Engineer and Design, 2014, 35(2): 440-444(in Chinese)
詹丽，姚国祥，强衡畅. 改进的基于 smartcard 的云用户双向认证方案[J]. 计算机工程与设计，2014，35(2)：440-444

[7] Das M L, Saxena A, Gulati V P. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 629-631

[8] Wang Y Y, Liu J Y, Xiao F X, et al. A more efficient and secure dynamic ID-based remote user authentication scheme[J]. Computer Communication, 2009, 32(4): 583-585

[9] Wen F, Li X. An improved dynamic id-based remote user authentication with key agreement scheme[J]. Journal of Computer Electrical Engineering, 2012, 38(2): 381-387

[10] Karuppiah M, Saravan R. A secure remote user mutual authentication scheme using smart cards[J]. Journal of Information Security and Application, 2014, 19(4): 282-294

[11] Gan Hong, Pan Dan. Research on dynamic ID-based remote user authentication scheme[J]. Digital Communication, 2014, 41(5): 1-5(in Chinese)
甘宏，潘丹. 基于动态身份远程用户认证方案的研究[J]. 数字通信，2014，41(5)：1-5

[12] Liu J Y, Zhou A M, Gao M X. A new mutual authentication scheme based on nonce and smart cards[J]. Computer Communications, 2008, 31(10): 2205-2209

[13] Huang H F, Liu S E, Chen H F. Designing a new mutual authentication scheme based on nonce and smart cards[C]// International Symposium on Parallel and Distributed Processing with Application, ISPA 2010. Taipei, Taiwan, 2010: 570-573

[14] Li C T, Hwang M S. A lightweight anonymous routing protocol without public key en/decryption for wireless ad hoc network [J]. Information Science, 2011, 181(23): 5333-5347

(上接第 192 页)

SPICE 客户端的时延会迅速趋于稳定，而未优化的客户端的时延趋于稳定的时间比较缓慢，在带宽充足(大于 5000kB/s)后双方差异越来越不明显。由此可见，优化后的客户端在普通带宽下播放视频表现会比较出色，这也是大多数的应用场景。

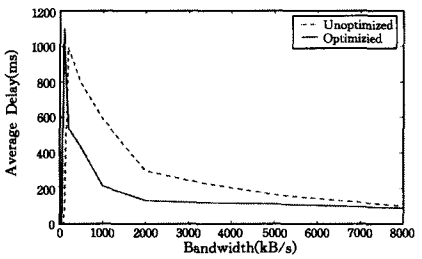

图 8 视频场景优化前后时延对比

结束语 通过分析 SPICE 机制以及某些场景下的特殊性，本着在不影响使用的前提下最大限度提高流畅度的原则，提出了在 SPICE 服务端和客户端之间构建探针通道，用以收集反馈信息，分别针对富交互和视频场景设计了不同的切换策略。实验表明，此方法可以在大多数情况下提升 SPICE 虚拟桌面在富交互和视频场景中的表现。

参 考 文 献

[1] Yu Tao, Bi Jun, Wu Jian-pin. Research on the Virtualization of Future Internet[J]. Journal of Computer Research and Development, 2015, 52(9): 2069-2082(in Chinese)
余涛，毕军，吴建平. 未来互联网虚拟化研究[J]. 计算机研究与发展，2015，52(9)：2069-2082

[2] Wu Jie, Kan Wen-xiao, Du Ran, et al. Application-oriented Virtualization Desktop Grid Architecture[J]. Computer Engineering, 2014, 40(3): 88-92(in Chinese)
武杰，阚文枭，杜然，等. 面向应用的虚拟桌面网格架构[J]. 计算机工程，2014，40(3)：88-92

[3] Zhang Jian-xun, Gu Zhi-ming, Zheng Chao, et al. Review of Cloud Computing Research[J]. Application Research of Computers, 2010, 27(2): 429-433(in Chinese)
张建勋，古志民，郑超，等. 云计算研究进展综述[J]. 计算机应用研究，2010，27(2)：429-433

[4] Simoens, Pieter, et al. Remote display solutions for mobile cloud computing[J]. Computer, 2010, 8: 46-53

[5] Xu Hao, Lan Yu-qing. Research on desktop virtualization technology based on SPICE protocol and its improvement solutions [J]. Computer Engineering & Science, 2013, 35(12): 20-25(in Chinese)
徐浩，兰雨晴. 基于 SPICE 协议的桌面虚拟化技术研究与改进方案[J]. 计算机工程与科学，2013，35(12)：20-25

[6] Qiao Yong. Research and Improvement of Video Transmission of SPICE in Cloud Desktop Environment[D]. Jinan: Shangdong Uiniversity, 2013(in Chinese)
乔咏. SPICE 协议的视频传输分析与改进[D]. 济南：山东大学，2013

[7] Schlosser, Daniel, et al. Improving the QoE of citrix thin client users[C]// 2010 IEEE International Conference on Communications(ICC). IEEE, 2010: 1-6

[8] Taylor, Cynthia, Pasquale J. Improving video performance in vnc under high latency conditions[C]// 2010 International Symposium on Collaborative Technologies and Systems(CTS). IEEE, 2010

[9] Massie, Thomas H, Salisbury J K. The phantom haptic interface: A device for probing virtual objects[C]// Proceedings of the ASME Winter Annual Meeting, Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems. 1994: 295-300

[10] Richardson, Tristan, et al. Virtual network computing[J]. Internet Computing, IEEE, 1998, 2(1): 33-38

[11] Orlov, Zigmund, Necker M C. Enhancement of video streaming QoS with active buffer management in wireless environments [OL]. http://oa.sloc.com.cn/handle/0/25468

[12] BhiogadeM S. Secure socket layer [J]. Ssrn Electronics Journal, 2001, 12(4): 475-490

[13] SPICE. Improving Spice performance: problematic scenarios and ideas [EB / OL]. (2015-09-10). http://www.spice-space.org/page/EnhancePerf

[14] Allman, Mark, Paxson V, et al. TCP congestion control [J]. ACM Computer Communications Review, 1999, 29(5): 308-309

[15] Chen Dan-wei, Zhang Zeng. A Feedback Frame-dropping Strategy of Improving SPICE Virtual Video Performance[J]. Computer Technology and Development, 2014, 14(1): 136-139(in Chinese)
陈丹伟，张增. 一种提高 SPICE 虚拟视频性能的反馈丢帧策略[J]. 计算机技术与发展，2014，14(1)：136-139

[16] Kim H J, et al. The QoE evaluation method through the QoS-QoE correlation model[C]// Networked Computing and Advanced Information Management. 2008

[17] Feng Jian, Ni Ming, Guo Zi-gang, et al. Design and Implementation of Cloud-desktop Based on Video Stream[J]. Computer Enginee-ring, 2013, 39(10): 37-41(in Chinese)
冯健，倪明，郭自刚，等. 基于视频流的云桌面设计与实现[J]. 计算机工程，2013，39(10)：37-41