基于 TEASE 管道技术的异构网络垂直切换安全认证算法*

赵 峰, 朱文强, 陈宏滨
(桂林电子科技大学 信息与通信学院, 广西 桂林 541004)

摘 要: 基于 WLAN 和 UMTS 构建的异构网络模型,提出一种适合该模型的垂直切换安全认证算法,用临时管道密钥(TTK)对数据进行加密,在接收端再用 TTK 进行数据解密。用平均切换次数、传输时延和丢包率三个指标评价所提出算法的性能。与已有垂直切换算法进行性能比较,其结果表明,提出的算法能有效减少切换次数,消除乒乓效应,减少传输时延和丢包率,可为实时业务所需的无缝切换提供有力保障。

关键词: 异构网络; 垂直切换; 安全认证; 乒乓效应
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2232-04
doi:10.3969/j.issn.1001-3695.2012.06.061

Security certification algorithm for vertical handoff in heterogeneous networks based on TEASE pipeline technique

ZHAO Feng, ZHU Wen-qiang, CHEN Hong-bin
(*School of Information & Communication, Guilin University of Electronic Technology, Guilin Guangxi* 541004, *China*)

Abstract: Based on a heterogeneous network model constituted by WLAN and UMTS, this paper proposed a security certification algorithm for vertical handoff in such a network. It used TTK to encrypt data and used TTK to decrept data at the receiver. Three indices, i.e., times of handoff, transmission delay and packet loss rate were adopted to assess the performance of the proposed algorithm. Compared with existing vertical handoff algorithms, simulation results indicate that the proposed algorithm can reduce the times of handoff effectively and eliminate the pong effect, reduce the transmission delay and the packet loss rate, and strongly support the seamless handoff for real-time services.

Key words: heterogeneous network; vertical handoff; security certification; pong effect

0 引言

近年来,我国移动通信网络技术发展迅猛,各种无线接入技术日新月益、层出不穷。未来的通信网络将不再由单一的网络构成,而是不同的无线接入技术的相互融合。异构无线网络中的移动切换分为水平切换和垂直切换[1]。水平切换指的是移动主机在基于同一种链路层技术的不同接入路由器间的切换;垂直切换指的是在不同的网络接口间的切换,通常在这个过程中,接入路由器和链路层技术也会发生变化。目前,通过移动和无线通信系统接入 Internet 的方式可分为两大类:a)基于蜂窝的接入技术,如 CDMA、GPRS 等;b)基于局域网的技术,如 IEEE 802.11WLAN,Bluetooth 等。WLAN 等局域网技术可以提供较高的带宽,但其物理覆盖范围非常有限;而 GPRS、CDMA 等网络具有消耗电量少、覆盖面积大的优点,网络连接基本上是随时可得的,但所提供的带宽却比较低。到目前为止,没有哪一种无线技术可以向移动用户同时提供低延迟、低功耗、低成本、高带宽以及高覆盖率的服务,因此,应该利用无线网络的融合来提高传输性能。但是,目前的切换技术大多针对水平切换,而垂直切换由于其特殊性和复杂性尚缺乏比较详尽和深入的研究;同时,对于如何保证移动节点跨网漫游的安全接入也是异构网络发展应用中不得不解决的一个难题。本文分析了现有的切换机制,提出了一种适合异构无线网络环境的垂直切换算法——基于 TEASE 管道技术的异构网络垂直切换安全算法。当移动终端进入两个网络重复覆盖区域时,移动终端接收到的信号强度发生变化,可以触发开始进行认证;当认证尚未完成时,通过旧节点生成临时管道(TTK),并把临时管道密钥分发给移动终端和新的接入节点,移动终端以旧节点为中转站通过 TTK 与新节点进行通信,从而保证了跨网切换过程中通信的连续和安全。从仿真结果中可以看出,使用管道的快速切换认证机制能显著地降低跨网切换过程中的认证延迟,也降低了数据丢失率,避免了可能产生的乒乓效应。因此,这种安全认证方式很适合用于实时应用中的切换。

1 现有切换技术分析

目前,国内外现有的切换技术基本上都是针对同一网络的水平切换,关于异构网络垂直切换这方面的研究成果还非常

收稿日期: 2011-10-19; **修回日期**: 2011-11-21 **基金项目**: 国家自然科学基金资助项目(61172055,61162008);广西自然科学基金资助项目(2011GXNSFB018072);广西教育厅科研项目(201012MS080)

作者简介:赵峰(1974-),男,山东日照人,研究员,博士,主要研究方向为无线通信技术;朱文强(1986-),男,湖南永州人,硕士研究生,主要研究方向为异构网络融合技术;陈宏滨(1981-),男,湖南邵阳人,副教授,博士,主要研究方向为传感器网络和认知无线电(chbscut@guet.edu.cn).

有限。

文献[2]介绍了支持最少切换延迟的无缝漫游连接。然而,文中是以降低扫描时间来减少切换延迟,并不适合于实时环境中。为了减少认证延迟,文献[3]提出了预认证机制。但该方法对预测新的接入点在 IEEE802.11i 中并没有作相关的定义,不准确的预测将会导致系统资源的浪费。文献[4]提出了频繁切换区的预测认证机制;文献[5]提出了多层次的多网融合垂直切换分析方法;文献[6]提出了一个叫做邻居图的结构来分析各移动接入点间的关系。为了进一步减少验证延迟,文献[7]介绍了四方握手的主动密钥分布机制,但该机制仍然有一些问题,包括多余重复的加载和资源的浪费。在文献[8]中指出了双向的信息交换能把延迟降低到最小,并可稳定在一个安全的水平。文献[9]介绍了基于 EAP-TLS 认证的异构网络融合无缝切换技术,由于切换过程中采用了 EAP－TLS 认证方式,使得切换的安全性得到了提高。文献[10]分析了传统的切换技术,提出了基于 MQoS 的切换算法,算法中采用了基于接收信号强度为标准的判决机制,一定程度上解决了乒乓效应的发生,但是这些都没有能够很好地解决切换时延过大的问题。文献[11]基于 WLAN 和 GPRS 的网络构建了一个简单的异构网模型,并提出了一种无缝切换控制方案来解决异构网垂直切换过程中可能遇到的时延过大、乒乓效应和业务阻塞等问题。

以上这些主要针对垂直切换策略和算法的研究,仍然不能完全解决垂直切换过程中的一些重要的问题,如传输时延过大的情况。此外这些机制并不能保证切换过程中数据传输的可靠性和安全性。

2　切换模型和安全认证算法

以目前应用最为广泛的 WLAN 和 UMTS 网络为基础构建一个异构网络模型,介绍本文所提出的这种异构网络垂直切换安全认证算法。

在构建的模型中,移动终端以一定的速率在 WLAN 网络中移动,当移动终端移动到两个网络重复覆盖区域时,移动终端感知到当前接入点的信号强度低于预设的值,移动通信过程可能很快就会被迫中断。因此,为了保证通信时所需的信号强度和通信质量,移动终端会切换到另一个可以提供更好信号强度的网络。

在认证机制中,当移动终端开始进行认证时,发送一个认证通知消息给 WLAN,同时移动与 WLAN 之间的通信仍然处于连接状态,WLAN 仍然可以与移动终端通信。收到验证消息时,旧的接入点触发生成临时管道密钥(TTK)[12],生成临时管道密钥后,WLAN 发送一个认证确认消息给移动终端,同时,WLAN 也发送一个管道设置消息给新的接入点。当收到旧接入点的认证确认消息后,移动终端和新接入点开始系统认证,当认证过程尚未完成时,移动终端为了保证通信的连续性,通过 TTK 与新接入点进行通信(犹如建立了一条专用的传输通道,当然这条传输通道是虚拟的)。当认证通过后,新的接入点和移动终端间就建立了正常的通信关系,与此同时,临时管道也就完成了其使命,自动地失效了。

下面是具体的安全认证算法伪代码。当检测到接收信号强度变化时,新的访问接入点的操作如下:

```
a) detect RSS
b) if DRSS < Hy then
c) start handoff( W-U)
d) start EAP-TLS authentication ( MN、NAP)
e) if it is secure
f) trigger the TTK( OAP)
g) ELSE keep connection
h) receive the data packet
i) decripts the data packet received( PTK_OAP)
j) decript DATA_PACKET_TTK
k) if data packet is modified THEN
l) drop the data packet
m) else
n) find the old access point's address of the corresponding MN
o) sends data packet to the old access point
p) end if
q) end if
r) end if
```

当接收到数据包后,旧的访问接入点的操作如下:

```
a) receive the data packet
b) decript the data packet ( PTK_OAP)
c) if the data packet is modified during the transmission then
d) drop the data packet
e) else
f) find the routing path to destination address of the data packet
g) send the data packet to the correspondent node
h) if MN enter the NAP completely
i) TTK is lose effect automatically
j) MN connect to NAP completely and safely
k) end if
l) end if
```

其中:RSS 表示接收信号强度;Hy 表示门限电平;MN 为移动终端节点;NAP 和 OAP 为新的节点和旧节点;PTK 为瞬时密钥;EAP-TLS 为安全传输扩展认证协议。提出的安全认证算法的整个流程如图 1 所示。

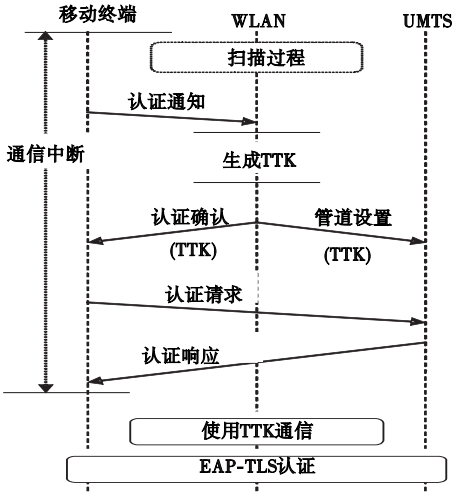

图1　提出的安全认证算法的流程

本算法以接收信号强度和最佳门限电平两者作为判决准则。其中接收信号强度(RSS)可从基站和 WLAN 站点直接得到,而门限电平可以用来消除乒乓效应,其取值 h_y 的确定可参考文献[13]。以 RSS 作切换指标时, WLAN 和 UMTS 的接收信号强度分别为

$$Rw = P_0 - 10n\log d + F(d) \tag{1}$$

$$Ru = K_1 - K_2\log(D-d) + v(d) \tag{2}$$

其中:d 和 $D-d$ 表示移动台到 WLAN 和 UMTS 基站的距离;P_0、n、K_1 和 K_2 表示路径损失参数;$F(d)$ 和 $v(d)$ 表示为与阴影衰落有关的静态零均值高斯白噪声过程, 且不相关。假定在

两个网络重复覆盖区域条件下，设 $P_0 = K_1, K_2 = 10n$，切换执行前后临界时刻的采样平均值最为关键，D_{RSS} 为临界点前最后一次采样均值与切换后第一次采样均值的差值，那么

$$D_{\mathrm{RSS}} = R_W - R_U = K_2 \log\left[\frac{D-d}{d}\right] + \tau \tag{3}$$

其中：$\tau = v(d) - F(d)$ 为零均值高斯白噪声过程，方差为 σ。当切换未执行时，$D_{\mathrm{RSS},1} = \alpha + \tau$，而切换执行后，$D_{\mathrm{RSS},2} = \beta + \tau$，为获得一个合理的门限电平，对任意的 D_{RSS}，设切换发生时事件为 Y，没有发生事件为 N，由全概率公式可知，发生切换时

$$P(D_{\mathrm{RSS}} | Y)P(Y) - P(D_{\mathrm{RSS}} | N)P(N) > 0 \tag{4}$$

另，

$$P(D_{\mathrm{RSS}} | Y) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(D_{\mathrm{RSS}} - \alpha)^2}{2\sigma^2}\right\} \tag{5}$$

$$P(D_{\mathrm{RSS}} | N) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(D_{\mathrm{RSS}} - \beta)^2}{2\sigma^2}\right\} \tag{6}$$

由式(4)可知：

$$\frac{P(D_{\mathrm{RSS}} | Y)}{P(D_{\mathrm{RSS}} | N)} > \frac{P(N)}{P(Y)} \tag{7}$$

令

$$\frac{P(N)}{P(Y)} = \xi \tag{8}$$

由式(5)(6)(8)可得 $\exp\left(\frac{(D_{\mathrm{RSS}} - \beta)^2}{2\sigma^2} - \frac{(D_{\mathrm{RSS}} - \alpha)^2}{2\sigma^2}\right) > \xi$，并可推出 $D_{\mathrm{RSS}} > \frac{\alpha^2 - \beta^2 + 2\sigma^2 \ln \xi}{2(\alpha - \beta)}$，取 $H_y = \frac{\alpha^2 - \beta^2 + 2\sigma^2 \ln \xi}{2(\alpha - \beta)}$ 作为切换过程的门限电平。

当移动终端进入两种网络的交叉覆盖区时，开始检测接收信号的强度。

1)从 WLAN 向 UMTS 切换　当移动终端感知到两种网络的接收信号强度相等时可以开始切换，当满足 $R_w = R_u - h_y$ 条件时，才开始切换过程，利用临时管道密钥对数据包进行加密，保证切换过程中通信的连续性和安全性，消除切换过程中可能导致的乒乓效应，具体如图 2 所示。

2)从 UMTS 向 WLAN 切换　原理同上。

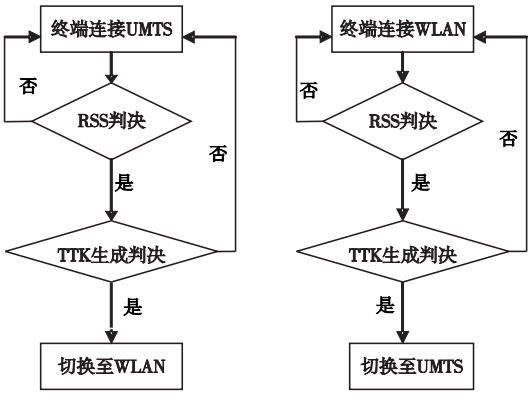

图2　切换过程示意图

3　仿真结果

本文采用 MATALB 7.0 仿真工具，对提出的基于 TEASE 管道技术的垂直切换安全认证算法和传统的垂直切换算法进行性能比较和分析。传统的切换一般是基于接收信号强度，根据接收信号强度的变化进行切换判决；而本算法是根据接收信号强度和门限电平进行初始判断，当感知到信号强度等初始条件变化时，通过生成 TTK 对传输的数据进行加密，进而保证切换过程中通信的完整与安全。假设 WLAN 接入点的覆盖范围约为 100 m，移动台以恒定速率 v 沿直线远离 WLAN 网络。$T_s = 0.01$ s 表示抽样周期，$T_0 = 1$ s 表示定时周期。当移动终端速率改变时，如果平均接收信号强度 $\overline{\mathrm{RSS}[k]}$ 大于 $\mathrm{RSS}_{\mathrm{th-in}}$ 时，移动终端执行移入操作。如果 $\overline{\mathrm{RSS}[k]}$ 小于 $\mathrm{RSS}_{\mathrm{th-out}}$ 时，执行移出操作。$\overline{\mathrm{RSS}[k]}$ 用来估计平均接收信号强度，表示如下：

$$\overline{\mathrm{RSS}(k)} = P_T - 10n\log(kd_s) + f(\mu, \sigma) \tag{9}$$

其中：P_T 表示发射功率；$d_s = vT_s$ 表示移动台的单位移动距离；$f(\mu, \sigma)$ 为零均值、标准方差的高斯随机变量，代表阴影衰落。其中，WLAN 的信号强度切换进入门限预定义为 $\mathrm{RSS}_{\mathrm{th-in}} = -82$ dBm，移出门限为 $\mathrm{RSS}_{\mathrm{th-out}} = -87$ dBm。用平均切换次数、传输时延和丢包率三个指标对算法进行评估。

1)平均切换次数

在 UMTS 和 WLAN 重复覆盖的区域中，移动终端从一个网络切换到另一个网络的切换次数被认为是衡量算法性能的主要指标。切换次数用 n_{handoff} 表示，代表移动终端的切换次数。通过计算移出和移入的数学期望[1,13]：

$$E[n_{\mathrm{handoff}}] = E[n_{\mathrm{移出}}] + E[n_{\mathrm{移入}}] = \sum_{k=1}^{k_{\max}} \{P_{\mathrm{移出}}[k] + P_{\mathrm{移入}}[k]\} \tag{10}$$

其中：$k_{\max}$ 为移动台 MN 切换的时刻索引。在两个网络共同覆盖区域下，当 MN 发生垂直切换时，只要条件满足就可切换至 UMTS 或 WLAN。可将这个过程用马尔可夫模型[14]来表示。$P_{\mathrm{WLAN}}[k]$ 为在时刻 k 移动台与 WLAN 相连的概率；$P_{\mathrm{UMTS}}[k]$ 为在时刻 k 移动台与 UMTS 相连的概率；$P_{\mathrm{WLAN|UMTS}}[k]$ 为在时刻 $k - T_0$ 移动台与 UMTS 相连，在时刻 k 移动台将连接 WLAN 的条件概率；$P_{\mathrm{UMTS|WLAN}}[k]$ 为在时刻 $k - T_0$ 移动台与 WLAN 相连，在时刻 k 移动台将连接 UMTS 的条件概率。

在切换性能评估模型中，假设切换的起始时刻移动台在 WLAN 中，即 $P_{\mathrm{WLAN}}[0] = 1$ 而 $P_{\mathrm{UMTS}}[0] = 0$，$P_{\mathrm{WLAN}}[k]$ 和 $P_{\mathrm{UMTS}}[k]$ 的递归式如下：

$$P_{\mathrm{UMTS|WLAN}}[k + T_0] = P_r\{\overline{\mathrm{RSS}(k)} < \mathrm{RSS}_{\mathrm{th-out}}, \sum_{j=1}^{J} \overline{\mathrm{RSS}(k_j)} < Q, T\_\mathrm{live}[k] < T_{\mathrm{HO}} | P_{\mathrm{WLAN}}[k]\} \tag{11}$$

$$P_{\mathrm{WLAN|UMTS}}[k + T_0] = P_r\{\overline{\mathrm{RSS}(k)} \geqslant \mathrm{RSS}_{\mathrm{th-in}}, \sum_{j=1}^{J} \overline{\mathrm{RSS}(k_j)} \geqslant Q, T\_\mathrm{live}[k] \geqslant T_{\mathrm{HO}} | P_{\mathrm{UMTS}}[k]\} \tag{12}$$

其中：$T\_\mathrm{live}[k] = \frac{\overline{\mathrm{RSS}[k+T]} - \beta}{D_{\mathrm{RSS}}}$ 表示按目前平均接收信号强度能够负载某种应用的持续估计时间；β 表示某种应用服务质量的需求；$Q = \frac{qL}{2}$，$L = \frac{T_0}{T_S}$ 表示能量门限，q 取比 $\mathrm{RSS}_{\mathrm{th-in}}$ 大的值；T_{HO} 表示切换时延门限。

由此可以得出状态转移概率：

$$P_{\mathrm{移出}}[k + T_0] = P_{\mathrm{UMTS|WLAN}}[k + T_0] P_{\mathrm{WLAN}}[k] \tag{13}$$

$$P_{\mathrm{移入}}[k + T_0] = P_{\mathrm{WLAN|UMTS}}[k + T_0] P_{\mathrm{UMTS}}[k] \tag{14}$$

本算法和传统切换算法的平均切换次数结果如图 3 所示。

从图 3 可以看出，在 UMTS 和 WLAN 重复覆盖区域中，与传统垂直切换算法相比，采用本文所提出的算法使移动终端的切换次数保持在 1 次，明显减少了切换次数，有效地避免了乒乓效应。

2)分组时延概率

在切换性能的评估中,用户可以通过分组时延来评估服务质量。平均分组时延的概率 p_{delay} 计算如下:

$$P_{\text{delay}}=\frac{\sum_{k=k_{\text{start}}}^{\overline{k_{\text{移出}}}}P_{\text{threshold}}[k]}{(\overline{k_{\text{移出}}}-k_{\text{start}}+1)} \tag{15}$$

其中:$P_{\text{threshold}}[k]$ 表示分组传输超过传输时延门限的概率;$\overline{k_{\text{移出}}}$ 是 $k_{\text{移出}}$ 的均值,是近似表达;k_{start} 表示移动台进入切换区域,切换首次触发时刻。

从图 4 的仿真结果可以看出,采用所提出的算法,分组时延概率远远小于采用传统的垂直切换算法。这是由于当移动终端在 WLAN 和 UMTS 重复覆盖区域时,一方面与新接入网络进行认证;另一方面通过现有网络利用管道技术仍可与原网络正常地通信,只有当移动台完全移出 WLAN 后,才与 UMTS 进行正常的通信,中间的过程是不间断的,也就不存在传输时延了。

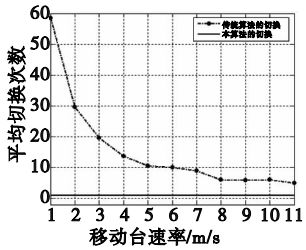

图3　移动终端的平均切换次数

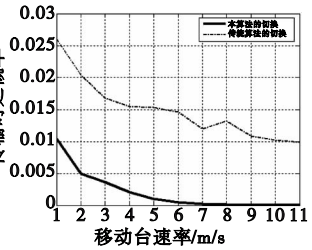

图4　分组传输时延概率

3)丢包率的分析

当移动终端跨网切换时,接收到的信号强度急剧变化或者低于预定的门限电平以下时,开始触发认证切换。通过 WLAN 网络生成临时管道密钥(TTK),移动终端通过 TTK 与 UMTS 网络进行间接的通信,丢包率计算如下[15]:

$$P_D(i)=\prod_{k=i-l}^{i}[P(\overline{\text{RSS}(k)}<R_{W_{\min}})(1-P_{ho}(k))] \tag{16}$$

其中:$l=\dfrac{\Delta T}{T_S}$,ΔT 为通信强阴影衰落下的保持时间。

$$P_{\text{ho}}(k)=\{P(\overline{\text{RSS}(k)}\leqslant Q_2)P(d\geqslant D)P[\sum_{m=k_0}^{k_0+M-1}\overline{\text{RSS}(m)}\leqslant Q_s]\} \tag{17}$$

其中:Q_2 表示 WLAN 的接收信号能量门限;Q_S 表示在一次切换过程中总的接收信号强度;d 和 D 表示移动台距 WLAN 和 UMTS 基站的距离;$k=k_0+M-1$;$R_{W_{\min}}$ 为 WLAN 网络中可以接收信号强度的最小值。

从图 5 可以看出,与传统的切换算法相比,所提出的算法由于使用了管道密钥对数据进行加解密,因此只有特定的可信节点能得到 TTK。除此之外其他节点任何情况下都不能获得 TTK,这样保证了数据传输的安全,数据在传输过程中没有任何的丢失。

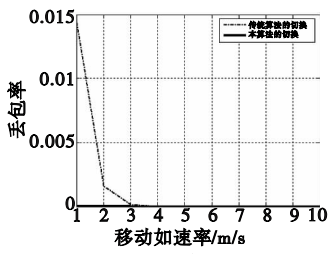

图5　丢包率对比

4　结束语

本文以 WLAN 和 UMTS 组建的异构网络为模型,提出一种基于 TEASE 管道技术的异构网络垂直切换安全认证算法,并采用平均切换次数、传输时延和丢包率三个指标来评价所提出算法的性能。仿真结果很好地反映了算法的性能,它能够减少切换次数,消除乒乓效应,降低时延和丢包率。

参考文献:

[1] 李军. 异构无线网络融合理论与技术实现[M]. 北京:电子工业出版社, 2008.

[2] VELAYOS H, KARLSSON G. Techniques to reduce the IEEE 802.11b handoff time[C]//Proc of IEEE International Conference on Communications. 2004:3844-3848.

[3] IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications[S]. New York: IEEE Standard 802.11, 2007.

[4] PACK S, CHOI Y. Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model[C]//Proc of IFIP Working Conference on Personal Wireless Communications. 2002:175-182.

[5] 方飞,李云. 无线异构网络的垂直切换判决算法[J]. 通信技术, 2010,43(6):137-139.

[6] MISHR A, SHIN M H, PETRONI N J, *et al*. Proactive key distribution using neighbor graphs[J]. IEEE Wireless Communications, 2004,11(1):26-36.

[7] KASSAB M, BELGHITH A, BONNINJ M, *et al*. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks[C]//Proc of the 1st ACM Workshop on Wireless Multimedia Networking and Performance Modeling. New York: ACM Press, 2005:46-53.

[8] MACCARI L, FANTACCI R, PECORELLA T, *et al*. Secure fast handoff techniques for 802.1x based wireless network[C]//Proc of IEEE International Conference Communications. 2006:3917-3922.

[9] HE Qing. A novel vertical handoff decision algorithm in heterogeneous wireless networks[C]//Proc of Interenational Conference on Wireless Communications, Networking and Information Security. 2010: 566-570.

[10] FRANCISCO J G P, JORGE O T. MQoS: a novel handoff algorithm for heterogeneous networks[C]//Proc of the 6th Columbian Computing Congress. 2011:1-6.

[11] 郭强. 一种无线异构网无缝切换控制方案及其仿真分析[J]. 上海交通大学学报, 2004,38(12):2026-2029.

[12] ZHANG Z, BOUKERCHE A, RAMADAN H. TEASE: a novel Tunnel-based sEcure Authentication SchemE to support smooth handoff in IEEE 802.11 wireless networks[J]. Parallel and Distributed Computing, 2011,71(7):897-905.

[13] ZAHRAN A H, LIANG B. Performance evaluation framework for vertical handoff algorithms in heterogeneous networks[C]//Proc of IEEE International Conference on Communications. 2005:173-178.

[14] 毛用才,胡奇英. 随机过程[M]. 西安:西安电子科技大学出版社, 1998.

[15] 刘侠, 蒋铃鸽, 何晨. 一种无线异构网络的垂直切换算法[J]. 上海交通大学学报, 2006,40(5):742-746.