

无线网络融合的安全 技术研究

Study on Security Technologies for Wireless Network Integration

冯志/FENG Min

(南京邮电大学 通信工程系, 江苏 南京 210003)
(Department of Communication Engineering, Nanjing University of Posts
and Telecommunications, Nanjing 210003, China)

摘要:融合多种网络可满足用户长时间连接和尽可能获得较高数据传输速率的需要,但融合后的网络也将各种网络的安全缺陷带进融合网络中。这不但给融合网络的运行带进各种原有的安全问题,而且增加了一些新的安全问题。对此,文章提出了基于恢复的多重防护解决方案,并使用公钥加密算法鉴权,使用私钥对通信数据进行加密。该方案可以为系统提供可靠的安全性,并实现用户对服务的不可抵赖性。该方案还处于研究起步阶段,下一步还需要明确各层的正确行为,以及出现多个恶意节点对某个合法节点诬陷时所应采取的行动。

关键词:无线网络;网络融合;安全方案;公钥

Abstract: Network integration brings users the satisfaction of long-time connection and maximum data rate, but it also brings security problems into the operation of integrated networks. Concerning this matter, the paper puts forward a recovery-based multiple protection solution. It uses public-key encryption algorithms for authentication and private-key for data encryption. This solution can provide reliable system security and avoid the deny of service of users. The study of this solution scheme is still in its initial stage. For the next stage, it must be solved that what correct actions should be taken at different layers when a legal node is attacked by multiple malicious nodes.

Key words: wireless network, network integration, security scheme, public key

中图分类号: TN929.5; TN918.91 文献标识码: A 文章编号: 1009-6868 (2006) 02-0040-05

随着移动通信技术的发展,网络正一步步向下一代移动因特网发展,即将蜂窝移动网络、自组网(Ad Hoc)、无线局域网(WLAN)等无线网络和有线因特网连接起来为用户提供“永远在线”、尽可能高速的数据速率以及动态的网络接入。然而这同时也带来一些安全问题,如漫游用户的机密性、接入控制和实体鉴权问题。

现阶段,对于无线网络融合的研究主要集中在任意两种网络的融合,主要的研究方向是蜂窝网络和WLAN及蜂窝网和Ad Hoc的融合。其中,蜂窝网络和WLAN作为已经较成熟的网络是目前网络融合中比较常用的方式,而蜂窝网络和Ad Hoc的融合由于Ad Hoc的自组织和自维护性能受到了广泛的关注。

WLAN由于其能够提供较高的数据传输速率被用来与蜂窝网进行融合,作为蜂窝网在热点地区的高速数据传输网,为用户提供高速数据服务。它通常作为蜂窝网的末端子网或可独立工作的网络,因此只需考虑网间的鉴权、切换等问题。蜂窝网络和WLAN相融合的主要系统是通用分组无线业务(GPRS)网与WLAN的融合以及通用移动通信系统(UMTS)与WLAN的融合。目前融合方案的重点主要放在

路由、切换等方面,实现安全的主要做法是在网络边缘设置网关。

由于Ad Hoc独特的结构特点,它与蜂窝网络的融合结构有多种不同方案。如:支持中继的蜂窝和自组织集成系统(iCAR)将Ad Hoc作为蜂窝网的补充来解决热点地区的网络拥塞,同时提高系统的频谱利用率,详细的系统结构见文献[1-4]。

统一的蜂窝与Ad Hoc网络(UCAN)与iCAR的思路相似,在数据传输速率降低时通过在信号较强的地方用代理机接收数据,并通过高速的IEEE 802.11协议向客户端发送数据来实现高速的数据连接^[5]。以上两种方法都是通过设置中央控制式网络的半固定节点为Ad Hoc节点提供一定的服务,其主要目的还是充分利用原有网络的资源。集成蜂窝与Ad Hoc转发技术(CAMA)的体系结构是借用了蜂窝网的“带外信号”,用蜂窝网的中央管理机制来提高Ad Hoc的网络管理和控制,从而提高Ad Hoc的性能,具体见文献[6]。这种方案是目前为数不多的充分利用Ad Hoc网络特点的网络,但是由于引入了蜂窝网络对其进行管理,除了最底层的Ad Hoc网络外,高层网络还是类似于中央控制式的网络。

而对于多跳蜂窝网(MCN)来说则是通过节点间的多跳路由将Ad Hoc多跳的路由接入方法引入蜂窝网络,使每个节点都参与到数据转发中来,这样可以减少基站数,增加覆盖范围^[7]。移动辅助连接实现(MACA)是一个动态信道分配机制,它也是在固定基站的蜂窝网中引入Ad Hoc转发技术。文献[8]中对这种融合方式有详细的叙述。这两种方案的主要特点是没有增加管理或是转发设备,仅通过对网络节点本身的修改来提高网络性能,但这同样也带来了更多的诸如鉴权、计费等问题。

1 网络融合面临的安全问题

不同的网络各有其相应的安全弱点,对于融合网络来说,除了构成网络的各个子网的安全弱点之外,不同网络的结合部位也是整个融合网络的安全弱点。

1.1 各种网络的安全弱点

对于蜂窝网来说,鉴权认证等基本的安全措施经过实际应用的检验已经比较完善了,但是在通信中传输的业务数据都是未经加密的明文。虽然,大部分的通信数据不涉及到机密信息,但是,还是有许多较机密的商业信息经由无线信道传输。这些数据可以被任何人通过监测无线信道获取。另外,即使安全性能较GSM好的CDMA网络也无法在扩频扰码等提供的一般的性能之外提供更进一步的安全保证。这种程度上的安全性能只能防止极低程度的信息泄漏如窃听,对于防止信道监听、流量检测等安全危害则无能为力。

WLAN与蜂窝网相似,任意节点在接入网络之前都要通过认证,否则该节点的数据将不允许在网络中传输。然而,与蜂窝网相同,WLAN传输的数据同样未经过加密,任意节点均能接收到其他节点发送的信息。如果恶意节点能够接入网络,就可以获得其他节点在网络中传输的数据,并利用这些信息危害发送端或接收端。

因特网的安全目前比较受关注。因特网由于其结构的开放性,很容易受到恶意攻击。IP安全协议(IPSec)、因特网密钥交互协议(IKE)等协议的提出为极不安全的因特网提供了一定的安全保证。IPSec的工作方式有两种,文献[9]中有详细的论述。利用了隧道技术的IPSec由于能提供较好的安全性,受到了广泛的关注,也被用在各种网络中以提供安全保证。但由于本身的固有缺陷限制了IPSec在其他网络中的应用。

Ad Hoc网络是分布式系统,无论是合法的网络用户还是恶意的入侵节点都可以接入无线信道,且所有节点既是终端也负责数据的转发,没有特定的可以部署鉴权的安全设备。因此,无线网络融合的安全方案首先要从安全性最差的Ad Hoc网络做起,网间的安全方案也要特别考虑到无特定安全设备的Ad Hoc网。因此,需要重点讨论Ad Hoc的安

全缺陷。

1.2 Ad Hoc网络的安全缺陷

Ad Hoc网络的特殊结构决定了它只能提供极差的安全性能,并且极易受到主动和被动的攻击。早期对Ad Hoc的研究重点主要放在了无线信道接入和多跳路由上,因此假设了一个友好且合作的环境。现在由于要潜在的一个敌对环境里为移动节点间提供受到保护的通信,安全问题已经成为了倍受关注的焦点。由于移动Ad Hoc网络(MANET)独特的特性给安全方案的设计带来一系列新的问题,如开放的网络结构、共享的无线资源、严格的资源限制和高度动态的网络拓扑。因此,现有的有线网络的安全解决方案并不能直接应用到MANET中。

由于Ad Hoc网络的安全问题一直未被深入研究,它的安全问题十分严重,已经成为实现Ad Hoc网的一个巨大障碍。Ad Hoc网络主要存在以下的安全性问题:无线链路使Ad Hoc网络容易受到链路层的攻击,包括被动窃听和主动假冒、信息重放和信息破坏;节点在敌方环境(如战场)漫游时缺乏物理保护,使网络容易受到已经泄密的内部节点(而不仅仅是外部节点)的攻击;分布式的网络体系结构使Ad Hoc网络的拓扑和成员经常改变,节点间的信任关系经常变化,与移动IP相比,Ad Hoc网络没有值得信任的第三方的证书的辅助,在节点间建立信任关系成为Ad Hoc网络安全的中心问题;通常Ad Hoc网络包含成百上千个节点,需要采用具有扩展性的安全机制。

本文认为还有一些其他的安全缺陷。由于Ad Hoc网络的开放性结构特点,因此,所有支持Ad Hoc工作方式的终端都可以接入到Ad Hoc网络中,或是说组成Ad Hoc网络。这就是说,别的网络的合法用户也可能成为Ad Hoc网络中的恶意节点,如出于节约终端能源的考虑而拒绝转发数据,或是为某种特殊的目的而将需要转发的数据复制后再转发出去,或是针对某个号码或是某个簇的恶意行为。因此,需要在多种无线网络融合的基础上,独立地考虑网间与各网络内部的安全方案。

1.3 网络融合带来的安全问题

融合后的网络不但融合了各种网络的优点,也必然会将各种网络的缺点带进融合后的网络中。前面所讨论的各种安全缺陷将或多或少地给融合后的网络运行带来各种安全问题。而且,融合后的网络在能提供更多样化的服务的同时也必将面临一系列新的安全缺陷,如网间信息的安全交互等。

Ad Hoc网络没有专门的安全认证中心,基于证书的加密鉴权方案中所需的可信赖的第三方是否能够在网络中以其他的形式代替,或是如何为Ad Hoc网络建立专门的安全中心是一个值得探讨的问题。另外,对于融合网络来说,

密钥和证书(包括业务提供商分配给用户的密钥和证书以及不同网络之间用来进行相互认证的密钥及一个网络的合法用户接入其他网络时临时分配的证书等)的传输也很困难。

2 无线网络融合的安全解决方案

对于由不同子网络融合而成的各种无线网络,它们的安全方案在一定程度上也是有差异的。

蜂窝网、WLAN等有中央控制的网络的安全方案较为简单。由于它们各自的安全性能在实际应用中已经得到一定的改善,仅需要考虑网络间的鉴权、认证。同时这些网络有专门的接入、路由设备,对于安全方案的部署有一定的硬件支持,仅需要在接入时由认证中心进行鉴权,路由安全方案则部署在路由设备上。这类网络的安全方案不但易于总结而且由于网络结构的原因易于实现。

本文的重点放在没有特定路由设备的Ad Hoc网络和蜂窝网络的安全方案上。由于Ad Hoc公开的对等网络结构、共享的无线资源、严格的资源约束和高度动态的网络拓扑等特点决定了可以应用于该网络的安全方案只需稍做简化即可应用于其他有中央控制的网络内。

2.1 网络融合方案的分类

近几年来,移动Ad Hoc网络(MANET)由于其自组织和自维护性能受到了广泛的关注。将Ad Hoc网络与蜂窝网络进行融合,Ad Hoc网络可以作为对蜂窝网络的有效补充。通过不同的融合方法,可以利用Ad Hoc的特点实现不同的功能。如iCAR、UCAN、MCN、CAMA等系统,都是基于不同的功能而设计出来的。

将各种不同类型且特性差异较大的网络进行融合,其路由、切换、鉴权和计费过程必须在提供各网络自身的路由、切换、鉴权和计费过程基础上实现。相对于路由和切换来说,鉴权是保证通信能够正常进行的前提,是所有功能实现的基础。而鉴权仅仅是安全问题的一部分,安全方案还必须保证通信过程中数据交互的安全。

融合方案在不考虑造价的前提下,可以分为3类:一是以蜂窝网为主干网,Ad Hoc网作为边沿子网辅助蜂窝网提供服务,这类方法主要是利用Ad Hoc来充分利用蜂窝网的频率资源;还有是用蜂窝网的带外信号对作为本地主干网的Ad Hoc网络进行管理,充分发挥Ad Hoc的优点,通过蜂窝网的集中控制使Ad Hoc工作得更加稳定;另外是在蜂窝网中引入多跳路由协议来减少基站数、增加覆盖范围,这类方法与第一种相似,但是对终端的性能要求比较高,能否投入实际应用还需要进一步探讨。

2.2 各种融合方案的安全弱点

首先确定这些网络的安全重点。以蜂窝网为主干Ad

Hoc为辅助的网络融合方案的安全重点是如何让合法的蜂窝网用户安全地接入到Ad Hoc网络,以及在接入Ad Hoc网络后如何在Ad Hoc网络内保证其通信安全。而以蜂窝网管理Ad Hoc网络的融合方案的安全重点是如何在Ad Hoc内部实现安全,以及蜂窝网管理Ad Hoc网络时如何安全地传输控制信息。另外,在蜂窝网中引入Ad Hoc工作方式则更需要对每个用户的身份信息进行更加严格的认证。安全重点可以归结为两大类:信令及信息的安全传输和对用户身份进行可靠的认证。我们认为只要解决了这两类关键问题,系统进行合适的配置就可以基本上保证用户信息的安全性。在这两类安全重点中,信令及信息的安全问题主要来源于Ad Hoc网络的开放性结构,因此工作重点将放在保证Ad Hoc网络的安全性上。

Tseng等提出的使用非对称加密技术的基于公钥的协议是防御性安全方案中安全性能较好的一种方案。本文利用这种算法结合文献[10]中提到的加强正确执行方式和多重防护的方法,以及结合文献[11-13]中应用IPSec提供安全保证的方法来总结一套适用于融合网络的保证信令和信息安全的结构。

2.3 安全策略

(1) 安全策略综述

本文提出的安全策略为:首先,要保证整个网络的安全就是要保证网络协议栈内各层的安全,通过对协议栈每一层的安全弱点的分析并加强相应的安全措施,来保证安全。同时也可以通过层与层之间的联系来实现对整个协议栈的保护。其次,对于未知攻击者的攻击方法是无法预先知道的,因此建立在这种不确定基础上的解决方案同样也是不可靠的。所以,本文认为对协议本身弱点的研究以及加强节点对协议规范的可靠执行是另一种更好的解决攻击的方法。第三,数据在传输中需要被加密以保证用户数据的安全,因此需要可靠的加密算法来对数据进行加密。目前公钥鉴权、私钥加密的方法广泛地应用于各个网络的安全方案中。因此,通过使用公钥算法的密钥进行鉴权并传输私钥加密算法的密钥不但可以提供较为可靠的安全性能,还能在数据量较大、实时性要求较高的通信过程中提供高效的数据加密,以达到用户对通信安全的要求,同时也不会给移动终端带来过高负荷的计算量。但是,对于长时间的数据连接来说,如何更新加密用的私钥以及如何确定更新周期则是另一个值得探讨的问题。

(2) 多重防护体系

已实际应用的网络安全技术已经比较成熟。对于多种网络融合后的安全,网间鉴权的实现以及能够保证Ad Hoc这种安全性极差的网络安全运行十分重要。对于各种集中式管理的网络来说任意两个网络间的网间鉴权方式是极为相似的,要推广到多个网络间的交互鉴权也是较为容易

的。况且在集中式管理的网络中有专门的路由设施,由于要由唯一的核网络向用户提供网络服务,在设置鉴权中心及部署鉴权等安全措施时都十分方便。如在接入时进行鉴权或是在需要服务时进行鉴权,安全方案可以部署在处理路由交换设备上,即由专门的设备负责系统的安全。而由于Ad Hoc网络分布式的网络特性,其安全方案则不能用这样的思路进行。

多重防护的概念是为了通过强制网络中的用户严格遵守协议规范来加强Ad Hoc网络的安全性能,同时本文认为这种模型也可以用于保证其他网络的安全。在每一层的每个功能块中包含了保证该功能块的功能正常实现的多个子模块,即将原有的各层功能细化以提高多重防护的可实现性。如网络层安全就是要保证节点转发时完全按照路由表的指示向前传送信息,不做出篡改数据包的下一条地址或在本地复制数据包等恶意行为;链路层安全就是保证正在通信的两个节点间的一跳连接。通过加密等方法来保证每个模块的安全性能需要较长的鉴权认证时间,而对于用户来说,这种时间当然越短越好。因此,本文觉得强化每个模块区分正确和错误操作的能力(或者明确哪些是符合协议规范的操作)可以防止Ad Hoc网络中的恶意节点入侵,或者说可以降低恶意节点对网络性能的破坏。这就是说,当某一节点的行为与规范不符时,其他节点可以对其身份进行怀疑,并强制其进行身份认证,同时报告可信赖中心。可信赖中心将其可信度参数值降低1,当这个参数降到某个特定值时,该节点将不作为转发候选节点,降到0时则被驱逐出网络。临近节点可以通过对网络上数据包的监听获得关于其邻居节点是否正确执行了协议规范。同时需要注意的是降低某一个节点的信赖度时需要多个节点对该节点的怀疑报告,以避免恶意节点对合法节点的陷害。另外,要充分利用Ad Hoc的自组织特性来构建网络,要求任意节点能够随时便利地接入网络,而这要求网络对节点的充分信任。本文提出的另一种方式则是假设每个移动节点第一次接入网络时都被当作为网络的可信赖节点,但信任等级较低,在选路的时候拥有较低的优先级。除一些特定情况外,均只将这些节点作为末端节点。每次有效地执行协议将为节点增加相应的信赖值,而一次或有限次误操作将会大幅降低信赖值。用这种方法来实现对恶意节点的容忍,并尽量降低恶意节点对网络的破坏。

对于不同网络间的鉴权可以由网络运营商事先签订漫游协议,以保证不同运营商的合法用户可以在各种网络间漫游并获得服务。在进入网络和需要取得服务前,用户用归属网络鉴权中心发放的证书向访问网络的鉴权中心发出请求,并通过归属网络的鉴权中心向访问网络的鉴权中心交互认证,确定该用户的合法性。当用户需要服务时利用其私钥对请求进行签名以保证服务的不可抵赖性。具体的过程可以参见文献[14]中的基于公钥的协议。

(3)数据加密技术

数据加密仅是安全协议中使用的工具,目前公钥算法能够提供较好的安全性,所以本文使用公钥加密算法来提高鉴权的可靠性以及服务不可抵赖性。但若是在通信过程中仍使用公钥加密算法,无疑加大了移动终端的计算量,这对于移动终端有限的计算能力来说是个严峻的考验。所以考虑到目前移动终端的计算能力,本文建议在鉴权时或通信开始时利用公钥算法内的参数来携带私钥或产生私钥的种子,这样在保证信息安全性的基础上也提高了加密的效率。

3 关键安全技术

3.1 安全方案

现阶段也有人对网络融合提出相应的安全方案。如Ala-Laurila等^[15]提出了通过GSM/GPRS和WLAN融合来支持移动用户的结构。然而,这个结构并没有考虑使用双接口(GSM/GPRS和WLAN)终端。WLAN作为3G的接入网络并直接连接3G网络的主要组成部分(如蜂窝运营中心)。两个网络共享相同的资源,如计费、信令和传输系统等。Luo等^[16]将3G和WLAN相融合为企业提供了Internet漫游解决方案。这个解决方案需要在合适的地方安放许多服务器和网关。虚拟专用网(VPN)的结构为企业提供了与3G、公共WLAN和专用WLAN之间的安全连接。

这些方案都只解决了一部分融合网络的部分安全缺陷,要完全解决整个网络的全部安全缺陷还需要进一步地深入研究。

3.2 加密技术

加密技术主要分为两大类:私钥加密技术和公钥加密技术。私钥加密的特点是加密和解密使用同样的或本质上相同的密钥对信息进行处理。这样就牵涉到密钥的传输和储存的问题,从而很难应用于开放式的网络结构中。而公钥加密技术牵涉到比较复杂的计算,但因为不涉及密钥的传输,相对地能够提供较好的安全性能。同时公钥加密算法还能够提供数字签名。因而,公钥算法可以给现代通信中的鉴权计费提供安全保证。

目前蜂窝网络中使用的加密方法都属于传统加密方法,即私钥加密技术。在信息交互过程中无论发送者还是接收者都使用相同密钥来进行数据加密、用户鉴权、验证数据完整性和数字签名。

3.3 密钥分配机制

本文希望利用公钥加密技术及IPSec、IKE的工作原理对用户的信息进行加密并对这些过程中使用的密钥进行分配。在接入、认证过程中使用公钥加密技术无疑可以提

供更高等级的安全性能,至于密钥的安全分发还是需要进一步探讨。对于有中央控制的网络来说,网络都有一个鉴权中心(AC),用户在接入网络之前需要向AC提出申请。由AC发放一个只有AC和用户知道的私钥,其对应的公钥则由AC向网络内的其他用户公布。而对于分布式的Ad Hoc网络来说,如果增加一个被所有节点信任的AC,则无法充分利用Ad Hoc的自组织特性,而自组织特性是提出Ad Hoc网络的主要目的。因此,如何在Ad Hoc网络中引入公钥加密算法是未来的重要研究课题。

至于在数据传输过程中的加密则应该尽可能地缩短数据加/解密时间,以支持实时业务并减轻移动终端的负担。在这方面,目前的加密技术中私钥加密技术能够提供比较好的性能。至于用于数据加密的私钥的传输则是另外一个需要考虑的问题。对于有中央控制的网络,私钥可以在鉴权时或是用公钥加密后传输,以确保私钥的安全性。目前主要的困难在于Ad Hoc网络中的私钥分发或传输。

至于路由的安全性,本文希望能够使用公钥加密技术(即基于证书的鉴权)来实现。在无需事先分配共享密钥接入网络时,基于证书的鉴权为通信团体验证实体提供了一种有力的手段。它需要使用证书产生数字签名,可以支持更复杂的业务模型。应用基于公钥的鉴权协议时,除了要进行与协议直接相关的计算外,校验者必须确认与之通信的实体的公钥证书^[17]。若在Ad Hoc网络中使用基于证书的认证,则认证者不但要认证单个证书的正确(如证书签名和合法时间的确认)和是否撤回,而且还要认证一条证书链路上所有的证书^[18]。对于路径的鉴权可以参见文献[19]中的方案。

应用IPSec是用通道模式保证多跳时的信息安全。由于传送模式较为方便,可以在Ad Hoc节点内存储其一跳的邻居,这样在一跳邻居间传输信息时可以用开销较小的传送模式进行工作。

4 结束语

本文针对多种网络融合的下一代网络提出了一个安全框架,即使用公钥加密算法鉴权,私钥对通信数据进行加密来提供基于恢复的多重防护解决方案。这个体系可以为系统提供可靠的安全性以及用户对服务的不可抵赖性。不过目前基于恢复的安全体系还处于研究的起步阶段,还需要明确各层的正确行为,以及出现多个恶意节点对某个合法节点的诬陷时所应采取的行动。

5 参考文献

- [1] Wu H Y, Qiao C M, De S, Tonguz O. Integrated Cellular and Ad-hoc Relay Systems: iCAR[J]. IEEE Journal on Selected Areas in Communications, 2001, 19(10): 2105-2115.
- [2] Qiao C M, Wu H Y. iCAR: An Integrated Cellular and Ad-hoc Relay System [C]//Proceedings of IEEE Ninth International Conference on Computer Communication and Network. Oct 16-18, 2000, Las Vegas, NV, USA. Los

- Alamitos: IEEE Computer Society Press, 2000: 154-161.
- [3] Wu H Y, Qiao C M. Quality of Coverage: A New Concept for Wireless Networks[J]. ACM Computer Communication Review (CCR), 2002, 32(1).
- [4] Wu H Y, Qiao C M. Modeling iCAR via Multi-Dimensional Markov Chains [J]. Mobile Networks and Applications, 2003, 8(3): 295-306.
- [5] Luo Haiyun, Ramachandran R, Prasun S, et al. UCAN: A Unified Cellular and Ad Hoc Network Architecture[C]//Proceedings of Annual International Conference on ACM Mobile Computing and Communications (MOBICOM 2003). Sep 14-19, 2003, San Diego, CA, USA. New York, NY, USA: ACM Press, 2003: 353-367.
- [6] Bhara B, Wu Xiaoxin, Lu Yi, et al. Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad Hoc Network (CAMA)[J]. Mobile Networks and Applications, 2004, 9(4): 393-408.
- [7] Lin Y D, Hsu Y C. Multihop Cellular: A New Architecture for Wireless Communications[C]// IProceedings of IEEE INFOCOM, Vol 3. Mar 26-30, 2000, Tel Aviv, Israel. Piscataway, NJ, USA: IEEE, 2000: 1273-1282.
- [8] Wu Xiaoxin, Biswanath M, Chan S H. MACA—An Efficient Channel Allocation Scheme in Cellular Networks[C]//Proceedings of Global Telecommunications Conference (GLOBECOM '00), Vol 3. Nov 27-Dec 1, 2000, San Francisco, CA, USA. Piscataway, NJ, USA: IEEE, 2000: 1385-1389.
- [9] Elkeelany O, Matalgah M M, Sheikh K P, et al. Performance Analysis of IPSec Protocol: Encryption and Authentication[C]//Proceedings of IEEE International Conference on Communications (ICC 2002), Vol 2. April 28-May 2, 2002, New York, NY, USA. Piscataway, NJ, USA: IEEE, 2002: 1164-1168.
- [10] Yang Hao, Luo Haiyun, Ye Fan, et al. Security in Mobile Ad Hoc Networks: Challenges and Solutions[J]. IEEE Wireless Communications, 2004, 11(1): 38-47.
- [11] Assaf N, Luo Jijun, Dillinger M, et al. Interworking Between IP Security and Performance Enhancing Proxies for Mobile Network[J]. IEEE Communications Magazine, 2002, 40(5): 138-144.
- [12] Qu Wei, Srinivas S. IPSec-Based Secure Wireless Virtual Private Network[C]//Proceedings of Military Communications Conference (MILCOM 2002), Vol 2, Oct 7-10, 2002, Anaheim, CA, USA. Piscataway, NJ, USA: IEEE, 2002: 1107-1112.
- [13] DaSilva L A, Midkiff S F, Park J S, et al. Network Mobility and Protocol Interoperability in Ad Hoc Networks[J]. IEEE Communications Magazine, 2004, 42(11): 88-96.
- [14] Tseng Yunmin, Yang Chouchen, Su Jiannhaur. Authentication and Billing Protocols for the Integration of WLAN and 3G Networks[J]. Wireless Personal Communications, 2004, 29(34): 351-366.
- [15] Ala-Laurila J, Mikkonen J, Rinnemaa J. Wireless LAN Access Network Architecture for Mobile Operators[J]. IEEE Communications Magazine, 2001, 39(11): 82-89.
- [16] Luo H, Jiang Z, Kim B J, Shankaranarayanan N K, Henry P. Integrating Wireless LAN and Cellular Data for the Enterprise[J]. IEEE Internet Computing, 2003, 7(2): 25-33.
- [17] Salgarelli L, Buddhikot M, Garay J, et al. Efficient Authentication and Key Distribution in Wireless IP Networks[J]. IEEE Wireless Communications, 2003, 10(6): 52-61.
- [18] Grecas C F, Maniatis S I, Venieris I S. Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration[J]. Mobile Networks and Applications 2003, 8(2): 145-150.
- [19] Kong Jiejun, Zerfos P, Luo Haiyun, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks[C]//Proceedings of Ninth International Conference on Network Protocols. Nov 11-14, 2001, Riverside, CA, USA. Los Alamitos, CA, USA: IEEE Computer Society Press, 2001: 251-260.

收稿日期: 2005-10-27

作者简介



冯志, 南京邮电大学通信工程在读硕士研究生, 研究方向为Ad hoc网络及其安全。