IPSec的多源多播组安全关联(GSA)管理机制的研究*)

韩秀玲[1,2] 王行愚[2]

(汕头大学工学院 汕头515063)[1] (华东理工大学信息技术与工程中心 上海200237)[2]

摘 要 GDOI是一个支持IPSec等数据安全协议保护多播应用安全的组密钥管理协议。本文首先论述了应用IPSec保护多播数据安全的重要意义,接着分析了GDOI协议的工作机制,并讨论了基于GDOI密钥管理协议的IPSec多播的安全性及其只适用于单源多播的局限性。根据IPSec协议的特点和多播应用的要求,提出了对GDOI协议的扩展建议,描述了扩展协议的工作过程,并基于用户主机完成了部分模拟实验。分析和实验说明该方案是可行的,扩展后的GDOI协议能够支持基于IPSec的多源多播。

关键词 IPSec,GDOI,组密钥管理,安全关联(SA),组安全关联(GSA),多源多播

Researching for Group Security Association(GSA)Management Mechanism of Multiple-source Multicast of IPSec

HAN Xiu-Ling[1,2] WANG Xing-Yu[2]

(Institute of Technology, Shantou Umiversity, Shantou 515063)[1]

(Center of Information Technology and Engieering, East China University of Science and Technology, Shanghai 200237)[2]

Abstract GDOI is a group key management protocol for IPSec and other data security protocols to secure multicast application. This paper first discusses the significance of using IPSec to secure multicast data security, then analyzes the mechanism of GDOI, and discusses the security of IPSec multicast based on GDOI key management protocol and its limitation that it can only be applied to single-source multicast. According to the characteristics of IPSec protocol and the requirement of multicast application, an extended proposal to GDOI is proposed. We describe the work procedure of the extend protocol and perform a part of the simulated test. The analysis and test show that this scheme is feasible, and the extended GDOI protocol can support the multiple-source multicast based on IPSec.

Keywords IPSec, GDOI, Group key management, Security Association (SA), Group security association (GSA), Multiple-source multicast

1 引言

多播是一种基于Internet的一对多或多对多的有效通信技术,多播方式由于能够大量节省网络带宽和发送者资源(发送者对每个报文只需发送一次,多播路由器会自动地转发报文到每个多播接收者)而使其得到了越来越广泛的应用,如多方会议、远程教育、视频点播、协同工作等等。但由于Internet的开放性和共享性,使得多播应用面临很多安全问题,如数据包的截获、篡改、重放以及欺骗和拒绝服务攻击等。与单播(即端对端的通信)相比,多播由于涉及的是一组用户,其安全问题具有更大的复杂性。能否将单播中的成熟技术引入到多播中来保护多播数据的安全,是人们正在研究的一个课题。众所周知,目前用于保护单播数据安全的一个可靠协议是IPSec[1],该协议由IETF(Internet Engineering Task Force)开发,可无缝地为IP协议引入安全特性,它利用加密、认证、封装等技术为数据传输提供高度的安全性,其中包括访问控制、完整性、数据源认证,重放保护及机密性。正是由于IPSec协议的安全性和在数据处理方面的有效性,人们希望IPSec也能够适用于多播,一方面解决目前多播所面临的安全问题,另一方面,也希望有一个统一的安全机制,使IPSec在保护单播的同时也能保护多播数据的安全,这样,既充分利用了IPSec的安全性和有效性,又减少了协议设计的重复性和复杂性。然而,由于现有的IPSec协议是使用IKE(Internet密钥交换)协议[2]作为密钥管理协议,而IKE只是一个端对端的密钥交换协议,用于在两个通信实体之间建立和维护一个安全关联(即SA,它是两个通信实体之间的一种协定,包括使用的加密算法、密钥、密钥生命期、协议、工作模式、安全参数索引等等),所以基于IKE的IPSec只能适用于单播环境。多播由于面对的是组用户,除了要求具有单播的密钥交换特点之外,为了保证完美向前(退出的成员不能访问未来的组通信)和完美向后(新加入的成员不能解密以前的组通信)的安全性,还需要支持组密钥的动态分配和更新,所以,不能简单地将已有的IKE协议作为IPSec的多播密钥管理协议。为了使IPSec的安全特性也能够适用于多播,近来一些研究团体或个人也提出了一些建议或方案,概括说来,其基本思想主要有两种:(1)修改IPSec协议本身,使它支持安全多播;(2)设计一个新的适用于IPSec安全多播的密钥管理协议,使原有的IPSec协议既支持单播又适用于多播。一般认为,后者是一种比较合理的方案,因为它仅仅需要在应用层设计一个合适的密钥管理协议,操作系统内核中的IPSec不用被修改就可

*)基金项目:国家自然科学基金项目(编号:69974014);教育部重点学科项目(00053)。韩秀玲 博士生,主要研究方向:计算机网络安全。王行愚 教授,博士生导师。

用于多播，保证了现有的 IPSec 实现不需要改变它们对安全关联数据库的存储或访问机制，使同一个 IPSec 协议既可用于单播又能用于多播，减少了协议设计的重复性和复杂性，并保护了已有的应用。一个国际化组织 IETF 正在致力于这方面的研究，并开发了一个组播密钥管理协议 GDOI[3]。GDOI 协议实际上是一个组安全关联(GSA)管理协议，它通过对组安全关联的管理实现对组密钥的管理。目前 GDOI 已成为 IPSec 等数据安全协议的组播密钥管理协议。由于该协议具有安全的组播密钥管理特性，因而保证了基于 GDOI 密钥管理协议的 IPSec 多播应用的安全。然而，通过对协议的进一步分析可知，虽然 GDOI 协议可为 IPSec 提供安全可靠的组播密钥管理机制，但其应用范围还存在着局限性，即只适用于单源多播的情况(如新闻发布、股票报价、视频点播等1-M 的多播)。随着网络及网络应用的不断发展，多源多播(如多方会议、远程教育、协同工作等 M-M 的多播)具有越来越多的应用需求，如何实现基于 IPSec 的多源多播是一个十分重要的研究课题，在过去的几年里，人们对1 对多的多播研究比较多，而较少涉及到多对多的安全问题，尤其是 IPSec 的多播安全。本文通过对 GDOI 协议工作机制的深入研究，结合 IPSec 协议本身的的特点，提出了对 GDOI 协议的扩展建议，描述了扩展协议的工作过程，并基于 Linux 主机对用户方的扩展功能进行了模拟实现。分析和实验说明扩展后的 GDOI 协议能够支持基于 IPSec 的多源多播，并具有可靠的安全性。

2 组安全关联管理协议(GDOI)

GDOI (ISAKMP Domain of Interpretation for Group Key Management)是由 IETF 组播安全工作组提出的一个组安全关联管理协议，支持组播密钥管理，并通过 GCKS(Group Controller/Key Server)[4]进行组密钥的自动更新。该协议运行在 GCKS 和组成员之间，为组成员安全地下载和更新密钥，从而保证多播组始终以最新的组密钥进行安全的数据通信。为了实现这一目的，GDOI 使用了两种协议：注册协议和密钥更新协议。注册协议以端对端的单播的方式利用 GROUPKEY_PULL 交换为通过认证的新成员下载当前的组密钥，密钥更新协议通过 GROUPKEY_PUSH 消息将更新后的组密钥以多播的方式“PUSH”(下推)给当前的组成员。如图1所示。

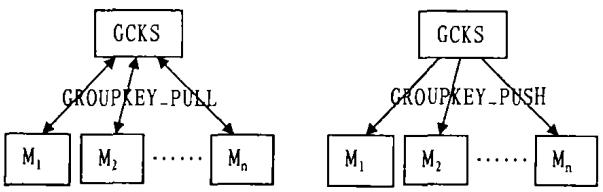

图1 GCKS 与组成员之间的密钥交换

为了能够安全地为组成员下载和更新组密钥，并保证组成员始终以最新的组密钥进行安全的组通信，GDOI 定义了一个组安全关联(Group Security Association，GSA)[4,5]的概念。

一个组安全关联(GSA)由三种不同类型的 SA 组成：注册 SA、密钥更新 SA(Re-key SA)和数据安全 SA(Date SA)，如图2所示。其中，GCKS 和每个组成员之间的 SA 为注册 SA，也称为“PULL”SA；GCKS 和所有的组成员之间的 SA 为密钥更新 SA(Re-key SA)，也称为“PUSH”SA；发送数据的成员和接收成员之间的 SA 称为数据安全 SA，也称为数据 SA(Date SA)。GDOI 正是通过对这三种类型 SA 的管理来实现对组播密钥的管理。

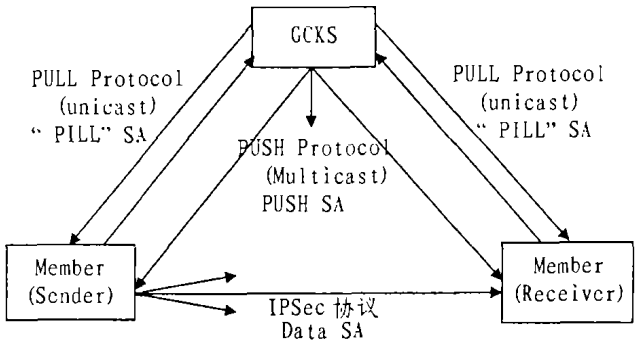

图2 组安全关联(GSA)模型

三种类型 SA 的特点及其之间的关系：

(1)注册 SA(即“PULL” SA)。一个新加入的成员为了通过认证并从 GCKS 获得组的加密策略(协议、加密算法、工作模式，密钥生命期等)、密钥材料(如密钥加密密钥(KEK)，组密钥(TEK))及安全参数索引(SPI)等，必须首先与 GCKS 建立一个安全关联，称为“PULL”SA，这是一个在 GCKS 与一个组成员之间单播通信的、由一个 IKE 阶段1定义的安全隧道保护的阶段2 的 SA[3]。由于它是从组成员发起的，所以也称为上拉 SA。PULL 交换的主要目的是为组成员安全地下载密钥，并建立和保护一个密钥更新 SA(Re-key SA)和数据安全 SA(Date SA)。

(2)密钥更新 SA(Re-key SA)，也称“PUSH” SA。组通信的一个特点是组成员的动态性，当组的成员发生变动时(有加入或退出时)，为了保证组播通信的安全，必须对组密钥进行更新，所以在 GCKS 和所有的组成员之间有一个“PUSH” SA，当组成员变动时，GDOI 通过 PUSH 协议(如 LKH 协议 RFC2627[6])将更新后的组密钥从 GCKS 下推(多播)给当前的组成员，从而更新 Data SA。

(3)数据安全 SA(Data SA)。GDOI 协议的最终目的就是为用户主机的 IPSec 等数据安全协议提供一个最新的 Date SA，从而保证组成员之间的数据通信安全。根据上述 GDOI 协议的原理，用户主机的 Data SA 是通过一个 PULL 协议来建立，并且通过 PUSH 协议进行更新。

一个 Data SA 的内容主要包括：目的地址、协议、加密算法、工作模式、组密钥、密钥生命期、安全参数索引(SPI)[7]等。在同一个多播组中，每个成员使用相同的组密钥及加密策略(协议、加密算法、工作模式，密钥生命期等)，但不一定使用相同的 SPI，所以每个成员的 Data SA 是否相同取决于他的 SPI 值。

3 基于 GDOI 密钥管理协议的 IPSec 多播的局限性

在单播 IPSec 中，根据 IPSec 安全结构 Internet 草案[RFC2401]的定义，通信双方在进行数据通信之前，必须首先建立一个安全关联(SA)，并保存在双方的安全关联数据库(SADB)中。一个 SA 由一个三元组(目的地址，SPI，协议)来代表[7]，其中协议为 ESP 或 AH。对于发送方，发出的数据包根据安全策略查询安全关联数据库中相应的 SA，并在数据包中填加该 SA 中的三元组(目的地址，SPI，协议)。在接收方，接收者仅仅根据接收数据包中的目的地址和 SPI 值判断一个 SA，即查找安全关联数据库，找出双方已协商好的相应的 SA，并按 SA 中的安全参数对数据包进行处理。在多播 IPSec 中，发送者与接收者之间的 SA 为 Data SA，Data SA 仍然以一个三元组(目的地址，SPI，协议)来代表，但其中目的地址为

多播地址，协议为 ESP。在同一个多播组内，由于目的地址和协议是相同的，所以在进行数据通信时，接收方也可以仅仅通过 SPI 来识别一个 SA，然后根据该 SA 提供的安全策略对接收的数据包进行处理。所以每个成员的 Data SA 是否相同，取决于他们的 SPI 值是否相同。

在同一个多播组中，为了保证 SPI 值不冲突，GDOI 协议规定每个成员的 SPI 值由 GCKS 负责分配（在用户注册时分配），协议共定义了两种 SPI 的分配和使用形式：(1)一个多播组使用同一个 SPI，因此每个成员拥有相同的 Data SA；(2)每个成员分配一个独立的 SPI，因此每个成员拥有一个独立的 Data SA。但通过分析可知，这两种 SPI 的分配和使用形式分别存在着下述的源认证、重放保护、Data SA 存储等问题，所以目前的基于 GDOI 密钥管理协议的 IPSec 多播只能适用于一个指定发送源的单源多播。

(1)第一种形式（一个多播组使用同一个 Data SA）

① 源认证问题。若一个组中有多个基于 IPSec 的发送源（实际上，一个多播组中的每个成员都可能是一个潜在的发送者），由于每个发送者使用相同的 Data SA，接收者仅仅知道信息来自于本组成员（可利用消息认证码执行基于组的认证），而不知道提交多播流量的明确发送者，因而无法实现源认证。

② 重放保护问题。根据对 IPSec 协议的分析我们知道，IPSec 协议（ESP 和 AH）的报头中包含一个强制的、单调增长的、提供一个抗重放攻击的序列号字段，在 IPSec 的多播通信中，组成员的计数器当 Data SA 被建立或更新时必须初始化到0，而每个发送者的第一个数据包的序列号一定为1。在单个发送者的情况下，数据包的序列号是单调增长的，接收者会根据这个序列号对接收的数据包进行处理和确认，因而使重放攻击失效。若一个多播组中有多个 IPSec 的发送者，在每个发送者使用相同 Data SA 的情况下，因为不能保证序列号的连续性和单调性，接收者将无法对来自不同发送者的数据包进行处理。为了保证接收方能够正确处理数据包，目前的 GDOI 协议规定，在多个发送源的情况下，从实施上保证接收者不执行 IPSec 报头中序列号的处理和确认，因而也就无法实现组成员之间应用数据传输的重放保护。

(2)第二种形式（每个组成员使用一个独立的 SPI）

这种方式下，每个组成员拥有一个独立的 Data SA，因此可实现源认证和重放保护，但它要求接收者必须存储每个发送者的 Data SA，由于一个多播组的每个成员都可能是一个潜在的发送者，所以 GDOI 要求每个接收者要存储相当于组成员数的 SA，这在一个大型而动态的多播应用中是不现实的。

由于这些问题的存在，目前基于 GDOI 密钥管理协议的 IPSec 多播在大型动态的环境下，只能适用于指定发送源的情况。如何解决多源多播的源认证、重放保护等问题，仍然是一个尚待研究的课题。

4 一种 IPSec 的多源多播解决方案

如上所述，GDOI 是通过对一个组安全关联的管理实现组播密钥的管理，它通过“PULL”SA 为新加入的组成员下载密钥加密密钥（KEK）和当前的组密钥（TEK），通过“PUSH”SA 对当前的组密钥进行更新，进而为组成员提供一个最新的 Data SA，然而，由于协议中没有定义对 Data SA 的进一步管理，所采用的两种 SPI 分配和使用形式存在着如上所述的问题，使得基于 GDOI 的 IPSec 多播不适用于多个发送源的情况。根据 GDOI 协议工作机制及 IPSec 协议的特点，本文提出了一种 IPSec 多源多播的解决方案，该方案通过扩展现有的 GDOI 协议对 Data SA 的管理功能，可解决 IPSec 多源多播情况下的源认证和重放保护等问题。

4.1 方案的设计与实现

根据以上分析，在一个多播组中，每个成员的 Data SA 是否相同取决于其 SPI 值，为了能够实现源认证和抗重放保护，这里要求每个成员拥有一个独立的 SPI，因而独立的 Data SA。同时，为了适应组成员的动态性和减轻用户方的存储负担，要求每个成员除存储自己的 Data SA 外，只动态地存储当前发送者的 Data SA（而不是所有成员的 Data SA）。一个发送者在发送数据之前，首先发送它的 SPI，接收成员收到一个 SPI 后，首先构造相应的 Data SA，并保存到 SADB 中，然后对接收到的包含该 SPI 值的数据包按相应的 Data SA 的处理规则进行处理。协议的描述如下：

1. 通过如前所述的 GROUPEKY_PULL 交换过程，一个新加入的成员从 GCKS 获得加密策略、密钥材料及 SPI 值，并建立一个 Data SA。

2. 当组成员发生变动（有加入或退出）时，通过 GROUPEKY_PUSH 消息将更新后的组密钥多播给组成员，从而更新每个成员的 Data SA。

3. Data SA 的管理。当一个成员要发送数据给多播组时，首先发送它的 SPI，由于一个组有相同的加密策略和组密钥，接收成员收到一个发送成员的 SPI 后，可根据组的加密策略和组密钥等参数构造该发送成员的 Data SA，并存放在安全关联数据库中。为了保证 SPI 传送的安全性和 Data SA 的有效性，组成员及 GCKS 要进行如下操作：

(1)组成员的操作

1)发送方

首先从 SADB 中取出他的 SPI 值，并用当前的组密钥对 SPI 值及身份信息加密，然后多播给组的其他成员：

发送成员→接收成员：$\{SPI, User\ ID\}_{TEK}$

其中 User ID 为用户标识，TEK 为组密钥

2)接收方

① SPI 的处理。用组密钥解密接收的数据包，获得 SPI 及发送者的身份信息，并与本机的 SPI 值比较。若不同，则接受该 SPI 值，然后构造一个 Data SA 并存入安全关联数据库。若 SPI 值相同，说明可能发生了冒充攻击，则立即多播一个冲突消息，使组成员放弃接受该 SPI 值；

② Data SA 的动态刷新。当组密钥（TEK）发生变化时，每个成员的 Data SA 将随 TEK 的变化而改变，所以设计上保证接收方 SADB 中每个发送者的 Data SA 随着 TEK 的变化而动态地刷新。

③ 应用数据的处理。当收到发送成员的 IPSec 应用数据包后，首先用组密钥解密，得到 SPI 值，并根据该 SPI 值查阅 SADB，找出有相应 SPI 值的 Data SA，然后根据 Data SA 中的安全参数对数据包进行处理。由于 SADB 中每个发送者的 Data SA 不同，接收者可同时接收多个发送源的数据而不产生冲突，并能根据 SPI 值及用户标识信息实现源的认证，同时，可根据 IPSec 报头中的序列号，实现成员之间应用数据传输的重放保护。

图3为组成员的 IPSec 主机上 GDOI 协议的扩展模块示意图，由于 GDOI 本身是一个应用层的协议，所以对它的扩展也只在应用层，扩展模块与 IPSec 内核的通信通过一个通信接口 PF_KEY 来实现，因为不涉及到网络层 IPSec 内核的改动，所以设计和实现方便灵活。

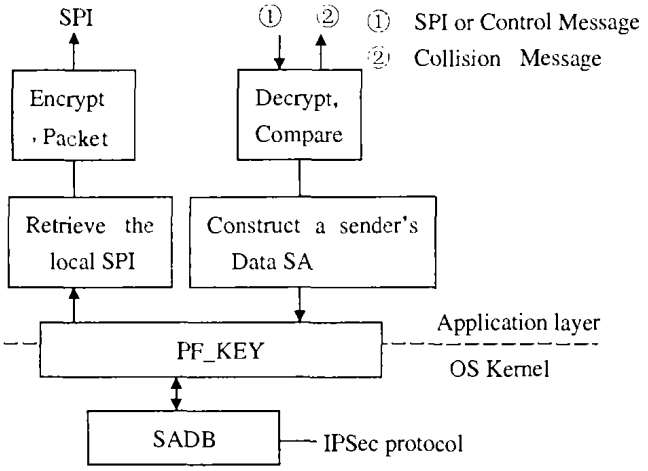

图3 用户 IPSec 主机上的 GDOI 扩展模块示意图

限于已有的条件，我们仅仅在用户方基于 Linux 主机利用手动方式对 SPI 的传送、Data SA 的构造、与 IPSec 内核的 SADB 之间的通信(包括 SPI 的检索以及 Data SA 的添加、更新、删除等)进行了模拟实验。PF_KEY[8]是一个新的 Socket 协议簇，用于实现应用层的密钥管理进程 IKE 与 IPSec 内核之间的通信。让 GDOI 的扩展模块利用这个 Socket 来发送和接收消息，实现了与 IPSec 内核的 SADB 之间的交互(如 SPI 的检索及 Data SA 的添加、更新、删除等)，(过程略)，从而验证了 Data SA 的可管理性。

通过在 SADB 中动态地存储不同 SPI 值的 Data SA，实现了对来自不同数据源的包含不同 SPI 值的数据包的处理。由于接收者的 SADB 中存储着每个当前发送者的 Data SA，所以可以基于 SPI 值及用户标识实现源认证和基于 IPSec 数据报头中的序列号实现重放保护。

(2) GCKS 执行的操作

1)一个新加入的成员在注册时，GCKS 也必须将当前发送成员的 SPI 值一道发送给该成员，使其 SADB 中能够存储当前发送者的 Data SA。

2)在 GDOI 的扩展协议中，GCKS 也同样作为一个接收者，但不接收和处理应用数据，只负责对发送者 SPI 值的安全验证和在发生异常情况时发出控制信息。在收到一个发送成员的 SPI 时，GCKS 查阅成员列表进行验证，若一个不良的组成员发送了一个伪造的 SPI，GCKS 将发出一个放弃接收这个 SPI 值的通知。由于 GCKS 只在发生 SPI 的伪造等异常情况时，才发出控制信息，因而不会增加通信的开销。

4.2 方案的安全性

(1)源认证：由于每个成员拥有独立的 SPI 及用户标识，因而接收者可以根据接收数据包的 SPI 值识别组内的明确发送者。

(2)应用数据的重放保护：由于接收者的 SADB 中存储着每个当前发送者的 Data SA，每个 Data SA 包含独立的 SPI 值，接收到的不同 SPI 值的数据包将会根据相应的 Data SA 来进行处理，因而保证了接收端的每个发送者数据包序列号的单调性和连续性，使系统可以基于 IPSec 数据报头中的序列号实现重放保护。

(3)SPI 的重放保护：在实现上保证不重复接收相同的 SPI 值。

(4)防伪造、截获和冒充：非多播组成员由于不知道组的通信密钥(TEK)，因而无法截获、伪造或冒充一个发送成员的 SPI 及应用数据；通过在 GCKS 方增加对发送者 SPI 值的验证，可防止组内不良成员的伪造；通过在用户主机增加对接收的 SPI 值的比较，可防止组内不良成员的冒充。

结束语 IPSec 是一个具有高度安全特性的数据安全协议，通过应用不同的密钥管理协议(如 IKE 或 GDOI)，可使已有的 IPSec 协议既适用于单播又可用于多播。为了使基于 GDOI 协议的 IPSec 多播进一步适用于多源的情况，我们对 GDOI 协议进行了扩展，增加了其对 Data SA 的管理功能，通过在用户方的 IPSec 主机上的模拟实验，验证了在多源情况下的 Data SA 的可管理性。分析和实验结果说明，通过对现有的 GDOI 组播密钥管理协议的扩展，可解决多源多播情况下的源认证和重放保护等问题。

本文的研究仅仅是解决多源多播安全问题的一个初步探索，实际上，多源多播是一个十分复杂的研究课题，要真正实现基于 IPSec 的多源多播，还有许多问题有待于进一步的研究和探索。

参 考 文 献

1 Kent S, Atkinsen R. Security Architecture for the Internet Protocol. RFC2401, 1998. 11
2 Harkins D, Carrel D. The Internet Key Exchange (IKE). RFC2409, 1998. 11
3 Baugher M, Hardjono T, Harney H. The Group Domain of Interpretation. Internet draft draft-ietf-msec-gdoi-07. txt, Dec. 2002
4 Baugher M, Canetti R, Dondeti L. Group Key Management Architecture. Internet draft draft-ietf-msec-gkmarch-03. txt, Fe-b. 2002
5 Hardjono T, Harney H. Group Security Association (GSA) Management in IP Multicast. NETWORKING 2002. 1123～1128
6 Wallner D M, Harder E J, Agee R C. Key management for multicast : Issues and architectures. RFC 2627, June 1999
7 Doraswamy D, Harkins N D. IPsec --新一代因特网安全标准. 北京：机械工业出版社，2000
8 McDonald D, Metz C, Phan B. PF_KEY Key Management API, Version 2. RFC2367, 1998. 7

(上接第25页)

3 Xylomenos G, Polyzos G C. TCP performance issues over wireless links. IEEE Communications Magazine, April, 2001. 52～58
4 Shah A. TCP Performance over Wireless Links. EE359-Wireless Communications, Autumn, 2001
5 Izumikawa H, et al. An Efficient TCP with Explicit Handover Notification in Wireless Nerworks. The Institute of Elexctronics, Technical Report of IEICE, Informantion and Communication Engineers, 2003
6 Perkins C, Ed. IP Mobility Support. IETF, RFC 2002, Oct. 1996
7 Xie Tiebing, Zhang Yu, Gao Jiming, Hou Ziqiang. A generic way for wireline and wireless access authentication. In: Intl. Conf. on communication Technology (ICCT 2003), IEEE Conf. 2003
8 Caceres R, Iftode L. Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments. IEEE Journal on Selected Areas in Communications, 1995, 13(5)
9 Hoe J C. Improving the Start-up Behavior of a Congestion Control Scheme for TCP. in ACM SIGCOMM, Aug. 1996
10 Barakat C, Altman E. Impact of Buffer Size on TCP Start-Up. In: Proc. of IEEE Middle East Workshop on Networking, Beirut, Lebanon, Nov. 1999
11 Fall K, Floyd S. Simulation-based Comparisons of Tahoe, Reno, and SACK TCP. ACM Computer Communications Review, 1996, 26(3): 5～21
12 范建华，等，译. TCP/IP 详解 卷一：协议. 机械工业出版社，2000
13 Lakshman T V, Madhow U. The performance of TCP/IP for networks with high bandwidth-delay products and random loss. IEEE/ACM Transactions on Networking, June 1997
14 Keshav S. A control-theoretic approach to flow control. In: Proc. of the ACM SIGCOMM '91, Sep. 1991. 3～15
15 The Network Simulator-ns2. http://www.isi.edu/nsnam/ns