第16卷 第8期
2006年8月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol.16 No.8
Aug. 2006

基于PGP信任模型的IEEE 802.16 Mesh网安全机制

孙炳龙,王国军
(中南大学 信息科学与工程学院,湖南 长沙 410083)

摘 要:IEEE 802.16是一种具有发展前景的宽带无线接入系统空中接口标准,但其安全机制仍存在不少问题,从而限制了其进一步发展。文中讨论了IEEE 802.16 Mesh模式中节点间的信任模型及建立连接的过程,并指出其中存在的安全漏洞。在此基础上,借鉴PGP中的自然人类社会的信任机制,改进了Mesh模式中节点间的信任模型,并提出了新的连接建立方式。分析表明新方式的安全性能要优于原方式。

关键词:IEEE 802.16;Mesh;信任模型;PGP;安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0239-04

Security Architecture of Mesh in IEEE 802.16 Networks Based on Trust Model of PGP

SUN Bing-long, WANG Guo-jun
(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: The IEEE 802.16 air interface standard has the potential to achieve great market success, but its security issues restrict its further progress. So describes the trust model of the Mesh mode in the IEEE 802.16 networks and the process of establishing links among the nodes in the Mesh mode. Then presents potential threats in this process. Furthermore, by using the trust model of PGP, modifies the trust model of the Mesh mode in the IEEE 802.16 networks, and also presents a new way to establish links among the nodes. Analysis shows that the new way is more secure than the original one.

Key words: IEEE 802.16; Mesh; trust model; PGP; security

0 引 言

IEEE 802.16是面向城域网范围的宽带无线接入技术的新标准[1,2]。作为当今业界最有前途的新技术之一,IEEE 802.16受到英特尔等许多大公司的强力支持,并陆续有相关产品上市。在安全方面为避免出现像IEEE 802.11设计之初的错误[3],IEEE 802.16工作组借鉴了已有的有线电缆数据服务接口规范标准(DOCSIS)中的安全思想[4]。DOCSIS是一个较为成熟的标准,在全球拥有大量的用户。然而,因为所处网络环境的不同,IEEE 802.16的安全机制仍然存在不少漏洞,特别是随着IEEE 802.16对移动性、非视距及Mesh模式的支持,其安全问题也越来越突出[3]。

文中首先简要介绍IEEE 802.16整体安全框架,分析Mesh模式中节点间的信任模型存在的安全漏洞;然后介绍了Pretty Good Privacy (PGP)系统中的信任机制思想,利用此思想修改了Mesh模式中节点间的信任模型,提出了节点间建立连接的新方式;最后分析比较了新旧两种方式的优劣。

收稿日期:2005-12-04
基金项目:湖南省自然科学基金资助项目(05JJ30118)
作者简介:孙炳龙(1980-),男,福建漳州人,硕士研究生,研究方向为无线网络安全;王国军,教授,研究方向为无线自组网、移动计算等。

1 IEEE 802.16安全机制

IEEE 802.16中通过在MAC层定义一个保密子层来提供安全保障。保密子层主要包括两个协议:数据加密封装协议和密钥管理协议。其中数据加密封装协议定义了两方面内容:

(1)IEEE 802.16支持的密码组件,如数据加密和认证算法;

(2)如何把这些加密算法运用到MAC层数据单元载荷中。

而密钥管理协议用来管理密钥的传播、更新等,维护其安全,如让基站(BS)把密钥安全地分配给用户站(SS)。

1.1 IEEE 802.16安全机制的主要工作流程

IEEE 802.16中节点加入网络要经过申请、认证等过程,进入网络后还要一直进行定期更新授权密钥(AK),维护传输加密密钥(TEK)状态机等工作,加强系统安全。其

中最为重要的入网申请认证过程,可概括成以下主要步骤:

(1) SS 向 BS 发送认证信息。认证信息包括 SS 设备制造商的 X.509 证书,此证书可能由制造商自己发布,也可能由第三方权威机构发布。

(2) SS 向 BS 发送授权请求信息。该信息包括设备制造商发布的 SS 设备的 X.509 证书、SS 支持的加密算法、SS 的基本连接 ID 号等。

(3) BS 根据上面两个步骤得到的两张 X.509 证书,验证 SS 的身份。如果验证成功,则为 SS 激活一个 AK。

(4) BS 将 AK 用 SS 的公钥加密后返回给 SS。

(5) SS 定时发送授权请求信息给 BS 来更新 AK。

SS 获得 AK 之后,利用 AK 向 BS 申请 TEK,再用 TEK 来对通信流量进行加密和解密,并维护一个 TEK 状态机,定时更新 TEK,同时也定时更新 AK。这就是 IEEE 802.16 基本的安全机制。然而从上述入网认证步骤可以发现,IEEE 802.16 只进行单向认证,也就是 BS 对 SS 进行认证了,可以保证 SS 身份的正确;而 SS 没有对 BS 进行认证,无法保证 BS 身份的正确,这样攻击者就可以伪装成 BS 对 SS 进行欺骗。不少研究者对此进行了讨论,并提出了一些改进方法[5,6]。

IEEE 802.16 支持点到多点(PMP)和 Mesh 两种工作模式,其中 Mesh 模式是一种新支持的模式。在 PMP 模式中通信流量只发生在 BS 与 SS 之间;SS 和主干网的通信及各 SS 之间的通信也必须通过 BS 来实现。而对于 Mesh 模式,通信流量除了发生在 BS 与 SS 之间,还可以通过 SS 来路由,各 SS 之间也可以直接通信[1]。增加对 Mesh 模式的支持,极大地扩展了 IEEE 802.16 的功能,然而也带来了一些潜在的安全威胁。下面对此进行分析。

1.2 Mesh 模式中节点间建立连接的过程

Mesh 模式中节点入网的过程与上述通用过程是一样的。而当节点入网后,它就可以和其它的相邻节点建立连接,其具体过程如下:

(1) 节点 A 发送一个挑战消息(Challenge),包括:HMAC{共享密钥,帧号,节点 A 的 ID,节点 B 的 ID}其中共享密钥是从 BS 得到的密钥,帧号为节点 B 发送的 MSH-NCFG 信息中的最后一帧的帧号。

(2) 收到挑战消息后,节点 B 也计算相同的式子,并比较值。如果值不匹配,则返回一个拒绝信息;如果值匹配,则同意建立连接,并返回一个挑战消息:HMAC{共享密钥,帧号,节点 B 的 ID,节点 A 的 ID}其中帧号是节点 A 在发出挑战消息时发送的 MSH-NCFG 信息的帧号。同时节点 B 随机挑选一个没有用过的链路 ID,来表示节点 B 到节点 A 的连接。

(3) 节点 A 收到信息后,计算(2)中式子的值,并比较。如果值不匹配,则返回一个拒绝消息;如果值匹配,则返回一个接收消息。同时 A 也随机挑选一个没有用过的链路 ID,表示从节点 A 到节点 B 的连接。

整个过程可以用图 1[1]来表示。

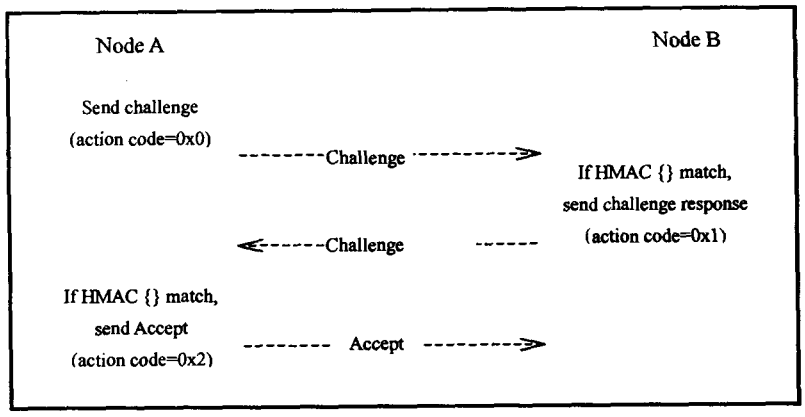

图 1 建立连接过程

Mesh 模式中,当相邻结点之间建立连接之后,节点要为每个连接维护一个 TEK 状态机。同时节点用共享密钥计算 HMAC-Digest,来加密密钥更新申请及回复消息,实现节点之间的相互信任。

从以上的介绍中,可见 Mesh 模式中节点间的信任模型存在一些潜在危险。首先,节点 ID 及帧号都是用广播的方式传播的,这些信息暴露在外,并无保密性。那么节点之间建立及维护连接只有共享密钥这个唯一的安全保障。但是在整个网络中所有的结点都共享相同的一个共享密钥,而且没有一个很好的更新机制,这样攻击者只要攻破任意一个节点就可以欺骗网络中的所有其它节点,将危害整个网络;同时如果内部有节点叛变,它将很容易欺骗网内其它节点而不被发现,即这种方式无法拒绝内部节点之间的相互欺骗。

针对上述问题,文中参考 PGP 系统中类似自然人类社会关系的信任机制,改进了 IEEE 802.16 Mesh 模式中节点间的信任模型,并修改了节点间建立连接的方式。

2 PGP 系统的信任模型原理分析

PGP 的信任模型是一个典型的以用户为中心的信任模型。在 PGP 中,一个用户通过担任证书签发者,对其他可信任的实体的公钥进行签名,同时使其自身的公钥被其他人所认证来建立并参加"信任网"。例如,当用户 A 收到一个据称属于用户 B 的证书时,发现这个证书是由他认识的用户 C 签署的,如果 C 是 A 的完全可信介绍人,则 B 的证书很可能就是有效可信的,如果 C 是 A 的部分可信介绍人,则 A 可采用相关策略决定是否要相信 B 的证书[7,8]。

2.1 相关术语

1)有效性:如果用户能够确信一个公钥证书属于正确的所有者,也就是说所有者拥有相关的私钥,则可认为该证书是有效的。

2)信任:指一个用户相信另一个用户能够签发有效的证书,信任是分级别的。

3)介绍人:如果用户 A 相信用户 B 能够签发有效的证书,就可以将 B 设为介绍人,此后所有经过 B 签名的证书,A 都可以认为是有效的。

4)元介绍人:指介绍人的介绍人。如果用户 B 被用户 A 设定为元介绍人,所有经过 B 签名的证书的持有者,A 都将认为是可信任的介绍人。

2.2 信任等级

PGP 系统中信任是分级别的,一般可分为完全信任、部分信任、不信任三个信任级别。信任级别主要是用来指导对于一个介绍人要给予多少信任,而用户实际上完全可以自己决定对一个介绍人的信任级别。

如果用户为某个公钥设定了信任等级,实际上就是指定了该公钥的持有者为自己的介绍人,所以信任的级别是针对介绍人而言的。信任级别的含义并不十分明确,主要是对介绍人应给予多少信任的一个大致指导,而且对于一个介绍人的信任级别可以完全由用户自己来决定。用户可以根据这样的原则来判断:用户将自己最信赖的朋友设为完全信任介绍人,将普通朋友设为部分信任介绍人等。这些简单的原则实际上就是用户的安全策略。

2.3 公钥有效性的判断

如何判断一个公钥是否可信,也就是公钥确实属于它的所有者,这是应用公钥密码的先决条件,也是任何公钥系统必须首先解决的问题。在 PGP 中,公钥的有效性能够被计算,也可以由用户自行设定。如果用户能够通过其它方式证明该公钥是真实的,就可以用自己的公钥对其签名,经过自己签名的公钥一定是有效的。否则就要对该公钥的介绍者的签名权重进行计算:如果至少一个签名具有终极信任的值(也就是元介绍人的签名),则此公钥是有效的。否则,对于完全信任的签名赋以权重 $1/X$,对于部分信任的权重赋以 $1/Y$,其中 X 和 Y 由用户设定(一般将 X 设为 1,Y 设为 2)。当所有介绍人的签名权重总和达到 1 时,此公钥被认为是有效的。因此,在没有终极信任的情况下,需要至少 X 个签名完全信任的或者至少 Y 个签名是部分信任的或者上述两种情况的某种组合。如图 2 所示。

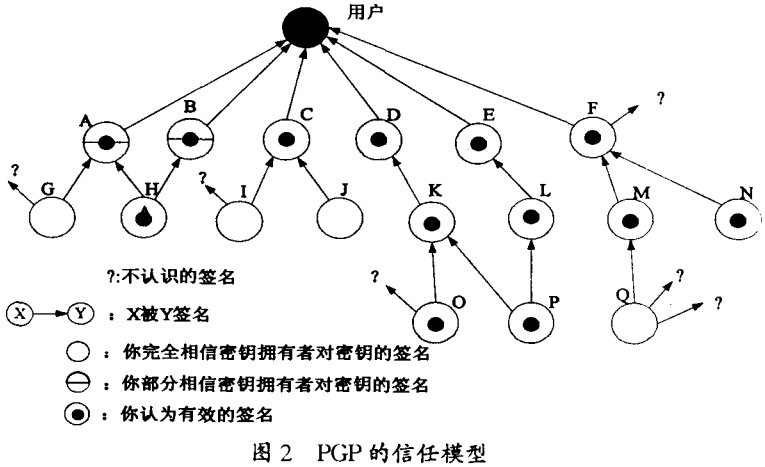

图 2　PGP 的信任模型

对于任何一个通过某种方式获得的公钥,PGP 总据上述条件判断其是否有效。如果是无效的,则将进一步的认证工作留给用户自己来完成。

3　改进的信任模型及节点连接方式

PGP 系统审慎的密钥管理、完善的信任模型,以及安全的加密算法,经过多年的发展,已经得到的广大用户的认同。PGP 现已成为一个公认的成熟的加密体系。在分析 IEEE 802.16 Mesh 模式的特点之后可以发现,它和 PGP 两者之间有着许多共同点:Mesh 模式是一种网状的拓扑结构,节点之间可以相互通信,节点之间的关系与 PGP 系统中用户之间的关系是类似的;Mesh 模式可以不要中心点的支持,这和 PGP 系统没有中心认证点也是类似的;Mesh 模式中两个相离较远互不信任的节点可能要建立连接,这和 PGP 系统中两个从未见面的用户可能要通信也是相似的。

所以完全可以借鉴 PGP 系统的安全思想,来改进 IEEE 802.16 Mesh 模式的信任模型,完善其安全机制。新的信任模型基于公钥加密体系,以网状信任模型为基础,网络中的节点对应于 PGP 中的用户,以公钥证书为节点的身份识别标志。节点之间进行通信,验证对方身份时,首先要利用文中介绍的策略判断对方节点是否可信。以节点 A 和节点 B 建立连接为例,具体的过程如下:

1) 节点 A 向节点 B 发送一个建立连接的请求消息,此请求消息还包括 A 的公钥证书、A 的 ID、B 的 ID 等其它信息。其中 A 的公钥证书已经被与 A 建立信任关系的节点签名。

2) 节点 B 收到节点 A 的消息后,首先检查 A 是不是可信任的节点(A 的证书是不是经过 B 的签名)。如果是可信任的节点,则同意建立连接,发送一个请求成功的返回信息。消息包括节点 B 的公钥证书、A 的 ID、B 的 ID 等信息。

如果节点 A 不是 B 的可信任节点,则查看 A 的公钥证书的签名者中有无 B 的可信任的介绍人签名,并计算相应权重,若权重小于 1,则返回一个拒绝连接消息。若权重大于等于 1,则表示 A 仍是一个可信任的节点,返回一个请求成功的消息。同时节点 B 向节点 A 的证书签名,并通知 A。

3) 节点 A 收到 B 的同意连接消息,检查 B 是否是可信任节点,其过程和上述(2)类似。若 B 是可信任的,则返回一个建立连接成功消息,并对 B 的证书进行签名,同意通知 B。若 B 是不可信的,则拒绝。

整个过程可以用图 3 来表示。

新的信任模型及建立连接的过程有效解决了原方式下的安全漏洞,使相邻结点建立连接过程更加安全可靠,具有很大优越性:

(1) 以公钥加密系统为基础,使用一些公

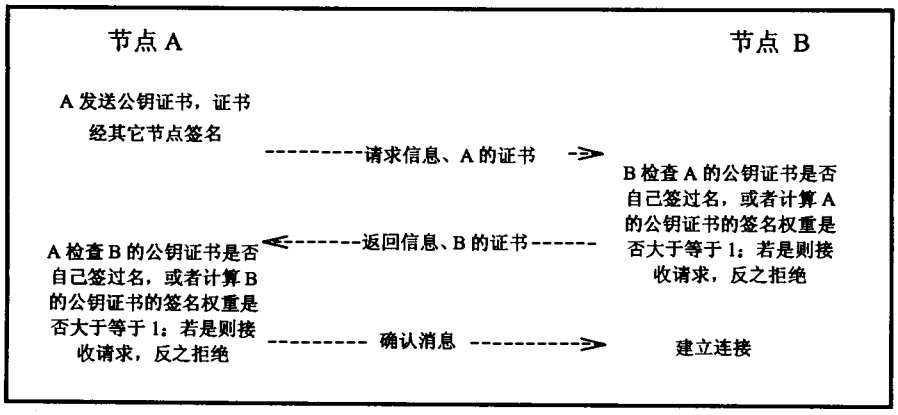

图 3 新的连接过程

认的成熟算法(如 RSA 算法等),其安全性能达到广泛的认同。

(2) 如果某节点的私钥丢失或被窃,并不会影响到整个网络的安全运行,只要及时公布、传递公钥证书撤销信息,就可以使其影响限制在很小范围内,同时新的信任模型可以有效防止内部节点的欺骗。

(3) 具有很好的可扩展性,将来也完全可以利用来解决各 SS 节点对 BS 节点的认证授权,这样既解决了原标准里的单向认证问题,也丰富完善了标准中的认证机制。

(4) 整个连接过程的认证过程不需要 BS 的支持与干预,没有中心支撑节点,避免了单点失效,增加系统稳定性。网状信任模型很像人类社会自然的信任关系,更加可靠、更加稳定。

新的方式具有突出的优越性,然而仍存在一些需进一步改进的地方:

①节点如何方便快捷地查询到其它节点的公钥证书。PGP 建议用户把自己的经过其它不同用户签名的公钥收集在一起,发送到一个公共场合,以方便用户查询、认证。

②公钥证书的注销问题。这是 PGP 系统及利用网状信任模型的系统中普遍存在的一个严重问题,即用户如何及时了解到某一个公钥证书已经失效,避免被欺骗。庆幸的是 BS 的存在可以较好地解决这些问题,也即,虽然 BS 对于 SS 之间通信不是必需的,但 BS 完全可以用来作为集中公布节点公钥证书和在线查询证书注销列表的地方,而且 BS 可以很方便地把证书注销信息及时通知到每个用户。

4 总 结

IEEE 802.16 是一种富有发展前景的新技术,将会是未来最重要的宽带无线接入技术之一。然而,其安全性能一直不能让用户完全放心,从而限制了其进一步的推广与发展。文中首先分析讨论了 IEEE 802.16 安全机制和 Mesh 模式中节点间信任模型及连接过程中存在的安全问题。然后借鉴 PGP 系统中信任模型的原理提出了新的信任模型与连接方式,较好地解决了这一问题。分析表明新方法要比原来的方法更为安全。下一步的工作将是,利用实验的或模拟的方式验证此方法的有效性;扩展 IEEE 802.16 的认证机制。

参考文献:

[1] IEEE. IEEE 802.16 - 2004. IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed Broadband Wireless Access System[S]. 2004.

[2] Eklund C, Marks R B, Stanwood K L, et al. IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access[J]. IEEE Communications Magazine, 2002,40(6):98 - 107.

[3] Johnston D, Walker J. Overview of IEEE 802.16 Security [J]. IEEE Security and Privacy,2004,2(3):40 - 48.

[4] Arbaugh W A. Wired on Wireless[J]. IEEE Security and Privacy,2004,4(1):26 - 27.

[5] Marks R B. Advances in Wireless Networking Standards[J]. Pacific Telecommunication Review,2002,4(2):30 - 37.

[6] 傅 坚.无线宽带固定接入系统的安全性分析[J].计算机工程, 2004,30(6):14 - 15.

[7] 刘海龙,张其善. PGP 中的信任问题及解决办法[J].北京航空航天大学学报,2003,29(3):278 - 282.

[8] Garfinkel S. PGP: Pretty Good Privacy[M]. [s.l.]: O'Reilly & Associates, Inc.,1996.

(上接第 238 页)

步的研究中,继续跟踪学习 IPSec 协议新标准,优化系统模块结构,寻求高速加密、认证算法,以提高系统的性能。

参考文献:

[1] Kent S, Atkinson R. Security Architecture for the Internet Protocol(RFC 2401)[EB/OL]. http://www.ietf.org/rfc/rfc2401.txt.,1998 - 12.

[2] Kent S,Seo K. Security Architecture for the Internet Protocol [EB/OL]. http://ftp.cc.ntut.edu.tw/ftp/Documents/Internet - Drafts/draft - ietf - ipsec - rfc2401bis - 06.txt., 2005 - 03.

[3] Doraswamy N, Hartins D. IPSec, 新一代因特网安全标准[M]. 京京工作室,等译.北京:机械工业出版社,2000.

[4] 汤 隽,李 超.基于 Linux 和 IPSec 的 VPN 网关[EB/OL]. http://linuxipsecvpn.cosoft.org.cn,2001 - 12 - 13.

[5] Yoshifuji H, Miyazawa K, Sekiya Y. Linux Ipv6 Networking past, present and future[A]. Proceedings of the Linux Symposium[C]. Ottawa, Ontario, Canada: [s.n.], 2003. 507 - 516.