

Ad hoc 网络及其安全性分析

刘志远^{1,2}, 杨植超¹

(1. 黄石理工学院 计算机学院, 湖北 黄石 435003;

2. 华中科技大学 计算机学院, 湖北 武汉 430074)

摘 要: Ad hoc 网络是一种特殊的多跳移动无线网络, 具有广泛的应用场合。文中介绍了 Ad hoc 网络的产生、定义、特点和应用, 然后在探讨 Ad hoc 网络的安全需求的基础上, 分析了移动 Ad hoc 网络易于遭受的攻击, 并集中讨论了移动 Ad hoc 网络的路由安全、密钥管理等关键问题。提出了按移动 Ad hoc 网络的安全需求进行分级, 然后分别实现的解决策略。

关键词: Ad hoc 网络; 安全策略; 路由协议

中图分类号: TP393.08

文献标识码: A

文章编号: 1005-3751(2006)01-0231-03

Ad hoc Network and Its Securing Analysis

LIU Zhi-yuan^{1,2}, YANG Zhi-chao¹

(1. School of Computer, Huangshi Institute of Technology, Huangshi 435003, China;

2. College of Computer Sci. & Techn., Huazhong Univ. of Sci. and Techn., Wuhan 430074, China)

Abstract: Ad hoc is a special multiple hop mobile wireless network which has broaden application fields. The paper firstly introduces the production, definition, characteristics and applications. Then, study the security goals to be achieved and the threats Ad hoc network faces. And focus primarily on the routing security and key management on Ad hoc network.

Key words: Ad hoc network; security mechanism; routing protocol

0 引言

随着信息技术的发展, 无线网络已经成为现代通信系统的一个重要组成部分。按照网络结构的差异, 将无线网络划分为有中心网络和无中心网络(又称 Ad hoc 网络)。在有中心网络中, 移动结点之间的通信必须通过固定的网桥(或者称为基站)转接, 常见的如蜂窝移动通信网络和无线局域网; 而在无中心的网络中, 结点间的通信并不需要固定基站的转接。

1 Ad hoc 网络的定义、特点及应用

1.1 Ad hoc 网络的定义

无线 Ad hoc 网络是由一组自主的无线节点或终端相互合作而形成的, 独立于固定的基础设施的并且采用分布式管理的网络, 是一种自创造、自组织和自我管理网络^[1]。与传统的蜂窝网络相比, 无线 Ad hoc 网络没有基站, 所有节点分布式运行, 具有路由器的功能, 负责发现和维护到其他节点的路由, 向邻居节点发射或转发分组。这种网络既可以单独运行, 又可以通过网关接入到有线骨干网络(如因特网)。Ad hoc 网络的起源可以追溯到 1968 年, 当时刚刚兴起对 ALOHA 网络的研究。ALOHA 的协议支持

单跳网络(网络中的每一个节点都可以到达所有其他的节点)的分布式信道接入, 但这最初用于固定网络节点。1973 年, DARPA 开始研究多跳的分组无线网络协议。多跳技术通过空间域的复用增大了网络的容量, 不过这需要更为复杂的路由协议来支持。过去 Ad hoc 网络主要用于战场和灾区这些无法或不便预先敷设网络设施的场合。现在, 随着新兴的无线技术如蓝牙技术的成熟, Ad hoc 网络的商用前景也越来越被看好, 各种便携设备如笔记本、移动电话、PDA、MP3 播放器的互联成为可能。

1.2 Ad hoc 网络特点

Ad hoc 网络与现有的通信网络相比有不同的特点:

(1) 在网络拓扑结构上, Ad hoc 网络具有动态的拓扑结构, 而现有网络的拓扑结构相对较稳定;

(2) 在传输带宽上, Ad hoc 网络的传输带宽有限, 容易引起网络拥塞;

(3) 在主机能源方面, Ad hoc 网络中的移动节点要依靠电池等可耗尽能源来提供电源, 而有线网络中则不需要;

(4) 在安全性方面, 虽然现有网络中也存在安全性问题, 但比较容易采取措施保护, 而 Ad hoc 网络面临更大的安全挑战;

(5) 与现有的通信网络相比, Ad hoc 网络生成时间短, 它是临时构建的, 使用结束后网络环境自动消失;

收稿日期: 2005-04-25

作者简介: 刘志远(1972—), 男, 湖北鄂州人, 博士研究生, 从事公钥密码, 网络安全和电子商务安全方面的研究; 杨植超, 教授。

(6) Ad hoc 网络具备相对现有网络更高的自我组织能力,不仅可以简化网络的管理,更能在处于动态的条件下如移动性、不确定的链接和无法预测流量负载的情况下,有效地使用网络资源;

(7) Ad hoc 网络采用分布式控制的方式,且网络不受固定拓扑结构限制,从而具有很强的鲁棒性和抗毁性。

1.3 Ad hoc 网络的应用

Ad hoc 网络具有广阔的应用前景。军事行动和地震、水灾或偏远地区的救援行动都是 Ad hoc 网络的传统应用领域^[2]。它也可以作为无线接入网,提供迅速的组网能力。在本地范围内,笔记本和掌上型电脑可以采用 Ad hoc 的方式在会议中发布和共享信息。采用蓝牙技术的个人局域网作为短距离的 Ad hoc 网络也极具发展前途。

2 Ad hoc 网络的安全目标

Ad hoc 网络的安全目标与传统网络中的安全目标基本上是一致的,包括:数据可用性、机密性、完整性、安全认证和抗抵赖性^[3]。但是两者却有着不同的内涵。

(1) 可用性。可用性是指即使受到攻击,节点仍然能够在必要的时候提供有效的服务。移动 Ad hoc 网络中,拒绝服务攻击可以在任何层次发起。如在物理层、数据链路层,入侵者能够通过填满有限的通信信道导致网络或服务不可用;在网络层,攻击者可以通过破坏路由协议,从而导致整个网络不可用。并且,移动 Ad hoc 网络拓扑的频繁变化、节点间信道的不可靠也对网络的可靠性提出严峻挑战。

(2) 机密性。机密性是保证特定的信息不会泄露给未经授权的用户。军事情报或用户账号等安全敏感的信息在网络上传输时必须机密、可靠,否则这些信息被敌方或恶意用户捕获,后果将不堪设想。路由信息在一些情况下也必须保密,因为这些信息可能被敌方用来识别和确定目标在战场上的位置。该问题的解决需要借助于认证和密钥管理机制。

(3) 完整性。完整性保证信息在传输过程中不被篡改。鉴别使接受者能够确定发送方的真实身份,防止伪装节点获取机密信息和资源,或者发送虚假的信息破坏网络和服务的可用性。

(4) 安全认证。每个节点需要能够确认与其通信的节点身份,同时要能够在没有全局认证机构的情况下实施对用户的鉴别。如果没有认证,攻击者很容易俘获某一节点,从而得以获取重要的资源和信息,并干扰其他节点的通信。只采用认证通常是不够的,认证只负责证明某人的身份,因此还需要通过授权来决定某种身份是否被允许做某些事情。由于 Ad hoc 网络没有固定的管理域,所以难以实施防火墙技术。

(5) 抗抵赖性。抗抵赖指发送方不能否定他所发送的信息,便于事后审计、检测入侵,并且能够预防内部攻击。

3 Ad hoc 网络路由协议安全分析

在 Ad hoc 网络中,移动节点同时起路由器的作用,发现并维持两个节点之间的路由。Ad hoc 网络路由协议的基本目的是在节点之间建立正确高效的路由,及时传递各种信息。如路由产生错误定向,会导致整个网络瘫痪,因此在整个网络安全中,路由安全起着举足轻重的作用。

Ad hoc 网络的路由协议中主要有宿节点排序的距离矢量路由协议(DSDV)、Ad hoc 按需距离矢量路由协议(AODV)和动态源路由协议(DSR)三种^[4-6]。DSDV 是基于 bellman - ford 路由机制的表驱动路由协议,该协议中每个移动节点都维护一个路由表,表中记录所有可能到达的目的节点及相应跳数。AODV 按需创建路由,可使广播路由的次数最少。AODV 不维护完整的路由表信息,不参与路由表交换,是按需获取路由的路由协议。DSR 与 AODV 的不同之处是当 DSR 进行路由发现时,先在缓存 cache 中查询是否存在相应的路由信息,为了减少路由发现时间,采用该协议必须配备大量的存储器。

Ad hoc 网络路由协议的安全需要考虑 3 个方面,即路由确定性、孤立恶意节点以及 Byzantine 鲁棒性。

(1) 路由确定性是指路由请求节点能够鉴别返回路由的正确性,并保证在路由存在的情况下发现路由信息;

(2) 孤立恶意节点指路由协议能够检测并排除恶意节点对路由的影响;

(3) Byzantine 鲁棒性指路由协议能够从恶意节点的破坏中自动恢复。

Ad hoc 网络路由协议的安全威胁来自两个方向:一是网络外部的攻击者通过发送错误的路由信息、重放过期的路由信息、破坏路由信息等手段,来达到致使网络出现分割、产生无效的错误的路由、分组无谓的重传,网络发生拥塞并最终导致网络崩溃的目的,攻击者还可以通过分析被路由业务流量来获取有用信息;二是网络内部的攻击者可以向网内其他节点发布错误的路由信息和丢弃有用的路由信息。两种攻击都能造成网络中合法节点得不到应有的服务,因此也可以看作为一种拒绝服务攻击。可以使用数据安全中的各种加密机制来解决第一种威胁,比如带有时间戳的数字签名。解决第二种威胁较为困难,对路由信息进行加密的机制不再可行,因为被占领的节点可以使用合法的私有密钥对路由信息进行签名。一种可行的方法是要求合法节点周期性地交换标识序列符,标志序列符由节点的标志符和序列号组成。占领某个节点的入侵者虽然能够获得合法的密钥,但他很难知道标志序列符,因此可以在一定程度上减少这种攻击带来的威胁。

4 Ad hoc 网络密钥管理

由于无线通信的无向性,Ad hoc 网络很容易造成信息的泄漏。因此,需要采用有效的保密措施来保证路由信息和数据的私密性。与任何其它分布式系统一样,正确使用密钥管理系统对于 Ad hoc 网络的安全性十分重要。在

Ad hoc 网络中,如采用单个 CA 建立密钥管理服务,负责整个网络安全的 CA 将成为整个网络的安全弱点。如果 CA 提供的服务不可用,节点将不能获得其他节点的公开密钥,不能与其他节点建立安全连接。备份 CA 能够缓解单点失效的问题,但是如果 CA 被入侵,将导致密钥管理系统的私密密钥泄漏,敌对方就能够使用该密钥签发错误的证书,并废除所有合法的证书,将给网络带来致命的威胁,而且简单备份 CA 提高了此种入侵的可能性。将信任分散是解决 Ad hoc 密钥管理的方法之一,基于门限加密机制的密钥管理服务是实现分布式信任的有效方法。

5 访问控制

在 Ad hoc 网络中同样存在控制对网络的访问以及控制访问网络提供的服务的需求。在网络层,路由协议必须保证不允许非授权节点加入网络,保证没有敌对节点加入和离开网络而不被检测到。在应用层,访问控制必须保证非授权用户不能访问服务。访问控制常与身份识别和认证相关联,确保合法用户有权访问服务。在一些系统中可能不需身份识别和认证,节点通过证书来访问服务。根据不同的网络结构和安全级别,访问控制的实现方式也不同。集中式的低安全级别网络,可以采用服务器控制的方式,用户 ID 加密码。对于战场情况,对网络和资源的访问控制都必须被定义。但是实现一个高效的、可扩展的、灵活的访问控制协议是非常困难的。

6 被俘结点的探测

在对安全敏感的 Ad hoc 网络应用环境中,由于节点容易受到攻击,被俘获的可能性也较大,因此必须要建立适当的信任机制,来保障 Ad hoc 网络的安全。在 Ad hoc 网络中,信任问题是中心问题,人们不能信任媒介,必须借助密钥。因此一个基本的问题是如何生成可信任的密钥而不依赖受信任的第三方。Ad hoc 网络是一个动态自组织临时网络,不能保证网络中各个节点持有被其他节点信任的公钥,并且它们也无法出示可以互相信任的证书,一种策略是允许节点之间委托信任,已经建立信任关系的节

点能够向组中其他成员扩展这种信任。但是,应该看到这种方法存在缺陷,因为它是以信任组为单位传递信任关系的,如果一个组中任何一个节点被攻击者俘获,而且这个被占领节点没有被其他节点发现的话,攻击者将威胁整个 Ad hoc 网络的安全。因此,为了增强安全性能,每个信任组中的节点必须定时互相认证,这种认证的频率不应太快,以减少网络开销。此外,如果一个节点要发送机密信息时,它可以主动发起认证过程,但是当网络的规模较大时,这种方式将会影响网络的性能。

7 结束语

Ad hoc 网络是一种特殊的网络,节点数量和类型可以是各种各样,应用的类型也是多种多样。不同的应用场合对于安全的需求并不一样,因此 Ad hoc 的安全措施应具有高度的灵活性、多样性和可扩展性,而且网络安全的能量消耗也应得到考虑。正确的做法是对于移动 Ad hoc 网络的安全需求进行分级,然后分别提出相应的解决策略。

参考文献:

- [1] 刘 剑,安晓波,李春生.无线网络通信原理与应用[M].北京:清华大学出版社,2002.386-407.
- [2] 米志超,郑少仁.无线战术互联网控制器通信协议的设计与实现[J].解放军理工大学学报,2000,1(6):24-29.
- [3] Ljubica B,Levente B,Srdjan C,et al. Self-organization in mobile Ad hoc network: the approach of terminodes[J]. IEEE Communication Magazine,2001,39(6):166-174.
- [4] Chen Z D,Kung H T,Vlah D. Ad Hoc Relay Wireless Networks over Moving Vehicles on Highways[A]. ACM Special Interest Group on Mobility of Systems,Users,Data and Computing[C]. California,USA:ACM Press,2001.247-250.
- [5] Zhou Lidong,Hass Z J. Securing Ad Hoc networks[J]. IEEE networks,1999,13:24-29.
- [6] Chung Weiho. Probabilistic analysis of routes on mobile ad hoc networks[J]. IEEE. Communications Letters,2004,8(8):506-508.

刊名变更启事

经国家新闻出版总署[2005]1066号文件批准,本刊自2006年开始,更名为《计算机技术与发展》,原刊号CN61-1204/TP作废,新编国内统一连续出版物号为:CN61-1450/TP。其它登记项目不变。邮发代号仍为52-127,页码增至232页。