第一图书网, tushu007.com

<<无线Ad Hoc网络安全>>

图书基本信息

书名：<<无线Ad Hoc网络安全>>

13位ISBN编号：9787302193371

10位ISBN编号：7302193371

出版时间：2009-3

出版时间：清华大学出版社

作者：（美）穆什塔瑞斯　著，钱权　译

页数：225

字数：334000

译者：钱权

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

前言

无线网路，无论是蜂窝网络还是无线局域网(LANs)，已迅速成为我们生活中不可或缺的一部分。
目前这种网络已广泛用于办公室、家庭、大学、飞机场和酒店的一些区域。
除此之外，小型无线设备(如PDA、移动电话、掌上电脑、建筑物上的一些小型设备以及传感器等)的广泛运用，使得无线Nirvana构想成为现实又向前迈了一步。
无线Nirvana是一种无缝的无线操作状态，它可使得任何无线设备能够在任何时候、任何地点，连接到任何其他无线设备或网络，以满足用户的需求。
显然，真正实现无线Nirvana还有很长的路要走。
无线移动自组网技术的发展，使得我们能够实现这一最终目标。
但是无线网络中涉及的安全问题，使得广泛采用这种网络仍存在很大障碍。
无线网络中的无线通信介质有很大的脆弱性，这些脆弱性很容易被利用从而实施对无线网络的攻击。
此外，无线自组网不能依赖传统的企业网络环境中的基础设施，如可靠的电源、高带宽、持续连接、公共网络服务、众所周知的成员身份、静态配置、系统管理和物理安全等。
因此，如果无线自组网没有足够的安全性，企业将避免使用它，政府机构也将禁止使用它。
同时，国防部门同样因其无法保证人员在战场环境的安全性，用户也可能未实施任何行为，而承担莫须有的责任，从而放弃使用无线自组网。
因此，要让无线自组网得到广泛的应用，解决其安全性问题是一个很重要的方面。
可以有两种方法。
一种方法是该领域的研究人员提出无线自组网安全的开放性问题，并提供解决方案，这样无线自组网的安全性可以不断得到加强。
尽管，让无线自组网更加安全，还需要做很多工作，但是经过数年的研究，已经取得了一些成果。
这其中，也包含我们的一些工作。
第二种方法是，直接向该领域的初学者介绍无线自组网存在的安全问题。
这样可让更多的人理解它，并且为扩展该领域的知识不断努力。
遗憾的是，很少有人沿着这个思路去做。
本书的重点就放在通过传播知识的方式介绍无线自组网中存在的安全问题。

第一图书网, tushu007.com

<<无线Ad Hoc网络安全>>

内容概要

无线Ad Hoc由于没有固定网络基础设施．具有组网灵活、移动性好等优点，在军事、交通、救援等多种场合有着非常好的应用前景。
然而，移动Ad Hoc的安全面临诸多挑战。
本书共8章。
全面系统地介绍了Ad Hoc网络安全的诸多方面，从基本安全理论、密钥管理、路由安全、入侵检测、安全策略管理以及节点定位安全等多个方面详细介绍了Ad Hoc网络安全．既有基础的理论．也有该领域最新的研究进展。
本书可供通信、计算机以及信息安全专业的大学本科生和研究生使用，对从事计算机网络安全工作的工程技术及研究人员也有学习和参考价值。

第一图书网, tushu007.com

作者简介

作者：(美国)Farooq Anjum (美国)Petros Mouchtaris 译者：钱权

第一图书网, tushu007.com

<<无线Ad Hoc网络安全>>

书籍目录

第1章 引言 1.1 无线Ad Hoe网络的定义 1.2 无线Ad Hoe网络的应用 1.3 无线Ad Hoe网络面临的威胁、攻击和漏洞 1.3.1 威胁 1.3.2 漏洞 1.3.3 攻击 1.4 本书概述第2章 基本安全概念 2.1 引言 2.2 基本概念 2.2.1 属性 2.2.2 密码原语 2.3 运算模式 2.4 其他安全属性 2.4.1 哈希链的单向属性 2.4.2 TESLA 2.5 小结第3章 密钥管理 3.1 引言 3.2 传统网络的解决方案 3.3 针对无线Ad Hoc网络的方案 3.3.1 基于非对称密钥的方法 3.3.2 基于对称密钥的方法 3.4 小结第4章 安全路由 4.1 引言 4.1.1 距离向量和链路状态路由 4.1.2 先验式与反应式路由 4.2 AODV协议 4.2.1 安全AODV协议 4.2.2 面向Ad Hoc网络的认证式路由协议 4.2.3 Ad Hoc安全感知路由协议 4.3 动态源路由协议 4.3.1 安全路由协议 4.3.2 Ariadne协议 4.3.3 EndairA：一个可证明的安全路由协议 4.4 DSDV路由协议 4.4.1 SEAD协议 4.4.2 SuperSEAD协议 4.4.3 S-DSDV协议 4.5 优化的链路状态路由协议 4.5.1 0LSR协议的安全扩展 4.5.2 安全链路状态路由协议 4.6 匿名路由协议 4.6.1 ANODR 4.6.2 MASK 4.7 针对路由的常见攻击 4.7.1 虫洞攻击 4.7.2 Rushin9攻击 4.7.3 Sybil攻击 4.8 小结第5章 入侵检测系统 5.1 引言 5.1.1 传统入侵检测系统 5.2 MANET中IDS面临的挑战 5.3 威胁模型 ……第6章 策划管理第7章 位置安全第8章 结论及未来展望缩略词参考文献

第一图书网, tushu007.com

章节摘录

插图：从安全角度来看，整个网络使用唯一密钥的方法是有问题的。
因为单个传感器节点被渗透就将破坏整个网络通信的安全性，而且难以选择性地撤销密钥。
要想在这种情况下保证安全性需要引入复杂的密钥撤销和密钥再生机制。
但是，考虑到通信时的能量消耗，这并不是一个好的选择。
而且，还需要有鉴定密钥再生过程的机制。
如果没有这些机制，将使攻击者能够远程再生密钥，甚至清除密钥。
但是，需要强调的是，文献[37]没有单个传感器节点被渗透的问题，因为文中假定传感器节点具有抗干扰能力。
不过，具有抗干扰能力的传感器节点会增加采用这种解决方案的代价。
共享对偶密钥的密钥管理方案能够避免由于单个密钥的泄露导致整个网络的通信被渗透的问题。
实际上，这个方案具有很强的弹性，任何一个节点被渗透都不会影响其他未被渗透节点间通信的安全。
然而，这个方案对传感器节点的存储空间要求太高，对于大规模网络而言该方案不可行。
举例来说，一个含有n个节点的网络，整个网络共有n(n一1)／2个密钥，而每个节点需要保存n一1个密钥。
那么，对于一个假设有10000个节点的网络来说是不现实的。
同时还要注意，由于只有邻居节点间才可能进行直接通信，所以其中许多密钥将不被用到。
由于节点通信范围和节点密度的原因，邻居节点的数量是有限的，所以网络中的所有节点不可能都是邻居节点。
这就会导致这样一种情况，一方面浪费节点存储空间，另一方面仍然要求节点具有很大存储空间。
这个方案还使得在已部署的系统中增加新节点要比最初部署时增加要难得多，因为这涉及为所有已部署节点更换上与新节点对应的新密钥。
给每个传感器节点重新分配新密钥的过程也增加了密钥管理的成本。

第一图书网, tushu007.com

<<无线Ad Hoc网络安全>>

编辑推荐

《无线Ad Hoc网络安全》是第一本针对无线自组网安全性方面的书，然而无线自组网安全性问题本身牵涉的内容很多，有安全网络协议、移动设备上的操作系统和各种应用等。
《无线Ad Hoc网络安全》的重点放在研究无线自组网的安全网络协议上，特别是无线自组网中两个设备通过无线接口进行相互通信时所涉及的安全问题。
《无线Ad Hoc网络安全》的宗旨是能够让读者明白无线网络安全领域的基本原理以及尚未解决的一些问题。
并希望不久的将来，在这个领域中取得更多的成就。
《无线Ad Hoc网络安全》对迄今为止无线自组网安全性问题的研究现状做了一个广泛而全面的概述，并讨论了各种解决方案的优缺点。
《无线Ad Hoc网络安全》适合各种水平的阅读者。
初学者可以从各种安全问题和解决方案的粗浅介绍中受益。
同时，通过将现有无线自组网的安全方面的重要成果汇编起来，可让初学者学习起来非常方便。
因此，《无线Ad Hoc网络安全》可以作为一本无线自组网安全性方面的教科书。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com