第33卷 第19期 计 算 机 工 程 2007年10月
Vol.33 No.19 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)19—0134—04 文献标识码：A 中图分类号：TP393

Ad Hoc网络保密与认证方案综述

胡荣磊，刘建伟，张其善
(北京航空航天大学电子信息工程学院，北京 100083)

摘 要：介绍了Ad Hoc网络保密与认证方案的最新研究进展。根据Ad Hoc网络的特性，对制定和实施保密与认证方案的关键问题进行了分析，按照单钥体制和双钥体制的分类方法，介绍和对比分析了现有的保密与认证方案，指出了各自的优缺点，对其中存在的主要问题提出了解决思路，并指出了进一步的发展方向。

关键词：Ad Hoc；保密与认证；密钥管理

Survey of Privacy and Authentication Schemes for Ad Hoc Networks

HU Rong-lei, LIU Jian-wei, ZHANG Qi-shan
(School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083)

【Abstract】 The article surveys the state of the privacy and authentication schemes for Ad Hoc networks, analyzes the important problems in establishing and implementing privacy and authentication schemes according to characteristic of Ad Hoc networks, introduces all schemes in existence and makes a contrastive analysis of their merits and faults, proposes some scenarios to solve problems that still exist in these schemes and presents the challenges that are still worth to further research in the area.

【Key words】 Ad Hoc; privacy and authentication; key management

1 概述

Ad Hoc网络是由一组带有无线网络接口的移动终端，在没有固定网络设施辅助和集中管理的情况下搭建的临时性网络。在制定Ad Hoc网络保密与认证方案时，必须要考虑它的结构特性和物理特性：

(1)无中心和自组织。PKI架构和TLS/SSL协议、Kerberos认证机制以及WLAN中的LEAP、EAP-TLS、SPKI、RAP-TTLS等协议[1]都不能直接应用在Ad Hoc网络中，这些方案都存在着单一在线的认证中心(certificate authority, CA)，CA的崩溃将造成整个网络无法获得认证。研究者们提出了各种不同的方案来解决这个问题。需要说明的是，Ad Hoc网络的“无中心性”并不等于没有认证中心。

(2)资源受限。Ad Hoc网络存储、计算以及通信能力的受限需要轻量级方案和协议的支持。美国国家标准与技术研究所(NIST)将Ad Hoc网络分成两类：移动Ad Hoc网络(mobile Ad Hoc networks, MANETs)和智能传感器网络(smart sensor networks, SSN)[2]，MANETs要求：1)算法简单，计算步骤少，节点间平衡；2)网络节点间信息流少，信息短；3)在工程实现上，要求占用存储空间小。SSN除了上述要求外，还要求具有可扩展性和错误容忍性。

(3)动态拓扑。动态拓扑给认证与密钥管理带来了困难，如在分布式认证模型中，如何保证任一个节点通信范围内有足够数量的认证节点问题。

2 保密与认证方案的阶段及分类

网络的阶段包括网络初始化阶段和网络运行阶段。在初始化阶段，网络节点获得网络运行必需的参数。这个阶段允许TTP(trusted third party)存在，其常见形式是认证中心(CA)或密钥分发中心(KDC)。在网络运行阶段，TTP不存在或处于离线状态，节点间地位平等，每个节点可以随时加入或脱离网络。认证阶段包含在网络运行阶段，完整的过程包括预认证、认证、认证信息更新、会话密钥建立、节点行为监控和节点隔离[3]6个阶段。在预认证阶段，节点通过安全信道交换认证信息，新节点加入网络时这个阶段同样存在，这是设计保密与认证方案的一个难点。认证阶段在非安全信道上进行，利用预认证过程中交换的信息来确定节点身份和建立安全信道。认证信息更新可以在每次认证后进行，也可定期 进行。

制定Ad Hoc网络保密与认证方案时，需要根据应用环境选择一系列的参数，根据这些参数可以对方案进行分类。这些参数包括单钥体制和双钥体制、MANETs和SSN、TTP的可用性、通信信道安全、平面拓扑与分层拓扑、网络中域的数量等。其中，TTP的可用性决定了保密与认证方案的总体设计思路，它包括3种情况：

(1)网络初始化阶段和有新节点加入时可用，完成证书、密钥或系统参数分发；

(2)网络初始化阶段可用，初始化阶段完成后，已有的网络节点将承担TTP的任务；

(3)任何网络阶段都不可用，自组织模型和无证书公钥模型即属于这种情况。本文根据密钥体制的分类方法，对Ad Hoc网络的保密与认证方案进行了介绍。

3 基于单钥体制的保密与认证方案

3.1 对密钥(pair-wise key)预分配

对密钥预分配方案克服了传感器存储空间小的缺陷，每个节点分配到总体密钥池中的一个子集，通过子集中的共享密钥建立安全信道，如果没有共享密钥，则要通过其他节点

作者简介：胡荣磊(1977－)，男，工程师、博士研究生，主研方向：无线网络信息安全；刘建伟，博士、副教授；张其善，教授、博士生导师

收稿日期：2006-10-13 **E-mail：**hrl@besti.edu.cn

建立一条安全路径。预分配方案有确定性[4]和随机性[5]两种形式，前者利用确定的过程构建密钥池和节点间的密钥链，后者从密钥池中随机选取密钥子集分配给节点，前者相对于后者能够提供更好的节点连通性。该方案在初始化阶段需要信任中心设置所有的传感器，所以，不能完全符合Ad Hoc网络动态拓扑性及无中心性的要求。

3.2 复活鸭子认证模型(resurrecting duckling)

该模型由F. Stajano和R. Anderson在 1999 年提出[6,7]，传感器节点之间短暂的连接过程，同鸭子从出生到死亡的过程非常相似。将传感器节点开始使用时刻看作是小鸭子“出生”时刻，将第 1 个给它发送密钥的节点作为它的“妈妈”，这个“子”节点受其“妈妈”节点的控制。这种认证模型类似于PKI的分层认证架构，如果主节点遭受攻击，属于它的所有节点都是不安全的。笔者建议在协议执行前密钥的发送使用物理连接，这在某些应用中是不现实的。

3.3 kerberos 辅助认证

kerberos认证的很多安全特性是Ad Hoc网络所需要的，比如阻止服务器和客户伪造身份、重放攻击检测、节点间安全通道建立等。Pirzada等提出了一种kerberos辅助认证方案Kaman[8]，在网络中设置多个kerberos服务器，服务器之间使用共享密钥定期进行安全的信息交换，以保证信息的一致性，节点认证需要先到服务器领取票据。这种方案虽然将kerberos的安全特性应用到Ad Hoc网络中，但增加了服务器节点的计算量和网络负荷，网络中有多个服务器都保存所有节点的信息，使得其安全性大大降低。

4 基于双钥体制的保密与认证方案

4.1 部分分布式CA(partially distributed CA)

部分分布式CA方案是由Zhou和Haas提出的[9]，方案采用分布信任机制和门限密码机制(n,t)，将CA私钥分成n份部分私钥，分发给n个指定节点，其中任意t个联合起来可以执行CA功能，签发证书时，CA节点生成部分签名证书，由一个联合节点重构完整的签名证书。Yi和Kravets的MOCA认证方案[10]对Zhou的方案作出了改进，取消了组合节点，并提出了证书撤销机制。部分分布式CA方案将单一的CA服务分散到n个节点中，有效地防止了单点失败，提高了网络的抗攻击能力。缺点是：

(1)节点需要到 t 个认证节点去申请证书，这些节点可能遍布于网络各处，需要多跳通信才能达到，增加了网络的通信负荷；

(2)认证节点的计算量和通信量都非常大，容易造成通信瓶颈；

(3)门限机制中的参数 n 体现了方案的可用性，t 体现了方案的安全性，选择合适的 n 和 t 并不容易。

4.2 完全分布式CA(fully distributed CA)

完全分布式CA方案[11,12]中CA的任务由所有网络节点共同承担，每个节点都持有部分私钥，任意t个节点联合可以执行CA功能，因此提高了系统的可用性。该方案的另一个特点是门限值可以在系统运行过程中随着网络节点数量的变化而动态改变，具有可扩展性。

这种方案的缺点是：

(1)证书的处理需要多个节点的参与，将部分签名组合成一个完整的签名计算比较复杂，因此效率并不是很高；

(2)方案假设每个节点周围都至少有 t 个节点，并不是所有情况下该条件都会成立；

(3)网络中的每个节点都是 CA 节点，攻击者可以攻击任意 t 个节点，从而降低了系统的安全性。

4.3 自组织认证(self-organization)

自组织认证是由Hubaux等提出的[13]，该方案基于PGP的思想，每个节点都有 2 个证书库：一个存储它向其他节点颁发的证书；另一个存储其他节点向它颁发的证书，当 2 个节点相互认证时，将 2 个证书库合并，找到一条认证路径。这种方案实现了完全的自组织，并且建立阶段比较简单。该方案存在的问题是：

(1)其认证基础是信任的可传递性，可传递性是有条件的，Hubaux的方案并不满足信任传递性的条件[14]；

(2)因为没有公认的可信第三方，所以建立的网络缺乏初始信任，攻击节点可以容易地加入网络；

(3)不能保证所有的节点之间都能执行认证，特别在网络建立初期，要达到能够 100%的认证，可能需要很长的时间。这种方法只适合应用于拥有大量节点的网络。

4.4 基于身份的认证(identity-based)

基于身份的机制[15]是用人们易读的(唯一的)身份标识作为公钥，这样身份是自认证的，节点不需存储公钥和密钥交换，降低了系统存储要求和网络通信量。Khalili等提出一个基于身份机制的密钥管理方案[16]，该方案与Zhou的方案相似，只是将分布式CA换成分布式PKG(private key generator)，所以其优缺点与Zhou的方案相同，此外，Khalili的方案仍存在的问题是：

(1)在 PKG 和用户之间没有安全信道的情况下，用户私钥很容易被攻击者窃听，PKG 如何识别请求私钥的节点，新节点如何安全地获得自己的私钥，文中没有讨论；

(2)基于身份的机制中有两种密钥：系统主密钥和用户密钥，为了系统的安全性，系统主密钥需要及时更换，对于系统功能而言这是非常关键的，该方案没有交代如何计算系统主密钥。Deng对Khalili的方案进行了改进，提出了一个比较完整的完全分布式方案[17]。

4.5 自认证公钥(self-certified public key)

自认证公钥的概念是Girault在 1991 年提出的[18]，公私钥对(sk,pk)由CA分发，CA将用户身份和自己的签名嵌入到用户的公钥中，验证方通过用户身份和CA公钥来确定被验证方公钥的合法性，即公钥本身具有认证功能，因此不需要证书或者其他机制提供认证，节省了带宽和存储空间。2004 年Merwe等为Ad Hoc网络提出一种门限自认证公钥分发协议[19]。

自认证公钥除了提供认证，还可用来协商密钥。Girault在他的文章中提出了基于 DH 算法的密钥协商协议，这个协议使用长期公钥来推导共享密钥，每次在两个相同的设备间执行协议都会产生相同的密钥，这是很不安全的，文献[20]中提出了使用自认证公钥生成短期会话密钥和组密钥的方法。

4.6 无证书公钥认证(certificateless public key)

这种方法包括所有使用公钥但不使用证书的方案。Demonstrative Identification[21]是一个典型的方案，方案假设通信双方以前没有任何联系，通过位置受限的可信通道(如红外接口、物理连接)交换预认证数据，设备间距离很短保证了信道和数据的可信性，利用预认证数据，通信双方在主信道进行传统的密钥交换。这种方案要求节点在有限的距离范围内，并且彼此信任，比如一个会议室内的所有人员，因此它不适合广泛分布的Ad Hoc网络。

5 基于单/双钥体制的保密与认证方案

5.1 基于口令(password)认证

口令是预先共享的秘密，在认证前通过安全信道进行交换，因此使用口令认证的前提是双方相互信任。口令认证通常希望口令比较短且容易记忆，但是这样的口令比较脆弱，不能抵挡强力攻击或字典攻击等，如果想从脆弱口令得到一个强密钥，必须引入非对称密钥机制。这种方法最早是由Bellovin和Merrit提出的[22]，他们使用口令加密一个短期公钥，提出了加密DH密钥交换协议，Asokan和Ginzborg在此基础上，结合超立方协议[23]提出了一个多方认证密钥交换协议[24]。该方案的缺点是计算量比较大。

5.2 基于 hash 链(hash-chain)认证

Hash链认证[25]的基本原理是：选择随机数x_0，利用hash函数对其进行连续n次计算$x_n=h^n(x_0)$，将x_n秘密发送到通信对方，保证x_0的秘密性。认证采用挑战－应答模式，节点通过应答hash链中x_i的前一个值x_{i-1}来证明自己的身份。基于hash链的认证协议很多，比较有代表性的是基于时间同步的广播认证协议TESLA[26]和uTESLA[27]：发方先将签过名的x_n发送到收方，发送数据包P_i时，利用hash链中的一个值x_j作为密钥，计算发送数据M的消息认证码MAC(M,x_j)，随同消息一起发送，在下一个数据包P_{i+1}中，公布x_j，并利用x_{j-1}做上述操作，收方收到P_{i+1}，利用x_{j+1}来验证x_j的正确性，然后用x_j验证数据包P_i的真实性，方案要求必须在收方收到P_i后，数据包P_{i+1}才能发送。Hash链方法计算量小，是设计轻量级协议的重要方法，适合于广播认证。Hash链只能提供单向的数据认证，身份认证需借助公钥体制来实现。

6 现有方案存在的问题及对策

除了上述方案外，基于簇的认证[28]也是一种重要的方法，它使认证和密钥管理设计起来比较灵活，能有效地适应Ad Hoc网络动态拓扑特性，但是该方案构建的是局部中心网络，并没有完全消除单点失败的隐患。

Ad Hoc 网络的应用多种多样，没有统一的保密与认证方案来适合所有的应用条件。表 1 对各种方案进行了比较。

表 1 Ad Hoc 网络保密与认证方案比较

体制	具体方案	理论基础	认证方式	有无 TTP	自组织性	资源要求	可扩展性	适用网络
单钥	对密钥预分配	×	通过共享密钥验证节点身份	初有①	不好	低	好	传感器
	复活鸭子模型	×	同上	有	好	低	好	传感器
	Kerberos 辅助	Kerberos	同 Kerberos	多个	不好	低	好	均可
双钥	集中式 CA	PKI	同 PKI	多个	不好	高	好	MANETs
	部分分布式 CA	门限密码	用系统公钥检验节点证书	分布式	一般	高	一般	MANETs②
	完全分布式 CA	门限密码	同上	分布式	好	高	好	MANETs②
	自组织认证	PGP 技术	通过证书链认证	无	好	高	好	MANETs②
	基于身份认证	Weil/Tate 对	利用身份标识认证用户身份	初有①	×	高	一般	MANETs
	自认证公钥	数字签名	用系统公钥检验用户公钥	初有①	×	高	一般	MANETs
	无证书公钥	×	用预交换的认证数据认证	无	好	高	一般	均可
混合	基于口令认证	×	口令	×	×	一般	×	均可
	基于 hash 链	杂凑函数	检验 hash 值	×	好	低	一般	传感器

注：①表示在初始化阶段有，在系统运行节点可以没有；②适合于拥有大规模节点的网络。

单钥体制方案对资源受限要求比较小，可扩展性好，是设计轻量级协议的重要方法，适用于 SSN。这种方案最大的问题是必须有 TTP 支持，最好的情况是只出现在网络初始化阶段，因此该方案的安全性不高。相对于单钥体制，双钥体制方案保密强度高，协议设计比较灵活，有较好的自组织性，但要求节点的运算能力强、资源受限程度小，比如 PDA 或手提电脑。从 TTP 的可用性分析，现有双钥体制方案采用两种方法：初始化阶段使用 TTP 和分布式 TTP，分布式 TTP 虽然有效防止了单点失败，但存在的问题也很多：(1)申请证书需要至少联系 t 个节点，增加了网络通信负荷，它实质上是牺牲了计算量和通信量来提高安全性；(2)只适合拥有大量网络节点的网络；(3)随着 Ad Hoc 网络规模变化，门限参数(n,t)需要及时调整，否则会影响网络的安全性和实用性，但现有的方案中都没有给出调整方案，导致其动态性能较差。

单/双钥体制方案中，双钥体制方案存在的问题它都存在，只是在计算量和通信量上要小一些。从以上分析可以看出，现有方案中存在的问题主要有以下几个方面：

(1)资源受限问题。双钥体制方案在现有方案中占的比例最大，但是所有方案对节点的资源受限要求都比较高，另外，多数方案再认证时的计算量和初次认证相同，这些都使得方案实用性并不好。可以用单钥体制或单/双钥体制来设计轻量级认证协议解决这个问题，比如对密钥预分配、基于 hash 链的认证等。

(2)TTP 和安全问题。TTP 的存在是为了方便节点管理和提高系统安全性，节点间通信要通过 TTP 来建立通信双方的信任关系。但是从 Ad Hoc 网络无中心性方面考虑，TTP 的存在是不合理的，并且也使得网络的安全性大大降低，各种认证方案对此做了不同的折中处理(参见表 1)。严格来说，这些措施都不能保证 Ad Hoc 网络的安全性，最安全的情况是无 TTP 或存在严格的离线 TTP，从这个角度来讲，在网络初始化时存在 TTP 是最合理的一种情况。

(3)初始信任问题。初始信任是指在网络运行阶段，当新节点加入网络时，如何确保这个节点的可靠性。在复活鸭子模型和无证书公钥模型中，通过位置受限的可信通道保证节点的可靠性；文献[12]中新节点证书只能由中心 CA 来颁发，这确保了每个证书的持有者至少向一个可信方成功地认证它自己。实际上这 2 种方法的条件是比较严格的，并不容易实现，其他的方案都没有提到这个问题。解决初始信任问题可以通过信任模型，节点可以计算通信对方的信任度，新节点信任度比较低，访问和控制能力有限，节点在交互过程中提高其信任度和访问权限，这样可以防止或减少恶意节点对网络造成的破坏。

(4)节点监控与节点隔离。这两个措施是保证网络安全的必要步骤，但是只有少数方案具有节点监控功能，比如文献[12]中的方案。许多基于证书的方案没有相应的证书撤销机制，比如部分分布式 CA 模型和自组织认证模型。可以制定相应的策略，使每个节点在网络运行阶段可以监视邻居节点的行为，当发现某节点存在问题时，废除其身份认证数据。

7 结束语

在 Ad Hoc 网络保密与认证方案设计上，其发展方向为：

(1)轻量级认证方案。

(2)自适应性和可扩展性方案。

Ad Hoc 网络本身具有动态拓扑性，要求保密与认证方案不应该是固定的，应当随着网络的变化动态调整。

(3)多点对多点的组密钥管理方案。

上述方案都是点对点的认证和密钥管理，在很多环境下要求多点对多点的通信，需要相应的密钥管理方案，目前在这方面所作的工作还很少。

(4)密码和安全新技术的应用。

椭圆曲线加密技术(elliptic curve cryptography，ECC)与RSA 相比，可用比较短的密钥实现同样的加密强度，因此计算速度比较快。基于椭圆曲线的组合公钥技术(CPK)以及可信计算技术等都为 Ad Hoc 网络的安全问题提供了新的思路。

参考文献

1 Kwang-Hyun Baek, Smith A W, Kotz D. A Survey of WPA and 802.11i RSN Authentication Protocols[R]. Dartmouth Computer Science, TR2004-524, 2004-11.

2 National Institute of Standards and Technology (NIST). Wireless Ad Hoc Network Projects[Z]. (2006-10). http://w3.antd.nist.gov/ wahn home.shtml.

3 Aboudagga N, Refaei M T, Eltoweissy M. Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues[C]//Proc. of ACM MSWiM'05, Canada. 2005.

4 Lee J, Stinson D R. Deterministic Key Predistribution Schemes for Distributed Sensor Networks[C]//Proceedings of 11th Annual Workshop on Selected Areas in Cryptography (SAC'04), Waterloo. 2004-08.

5 Eschenauer L, Gligor V D. A Key-management Scheme for Distributed Sensor Networks[C]//Proc. of the 9th ACM Conference on Computer and Communications Security. [S.l.]: ACM Press, 2002: 41-47.

6 Stajano F, Anderson R. The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks[C]//Proceedings of the 7th International Workshop on Security Protocols. [S.l.]: Springer-Verlag, 1999: 172-194.

7 Stajano F. The Resurrecting Duckling — — What Next?[C]// Proceedings of the 8th International Workshop on Security Protocols. [S.l.]: Springer-Verlag, 2000: 204-214.

8 Pirzada A A, McDonald C. Kerberos Assisted Authentication in Mobile Ad-Hoc Networks[C]//Proc. of the 27th Australasian Computer Science Conference. 2004.

9 Zhou L, Haas Z J. Securing Ad Hoc Networks[J]. IEEE Network Journal, 1999, 13(6): 24-30.

10 Yi S, Kravets R. MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks[C]//Proc. of the 2nd Annual PKI Research Workshop. 2003-04: 28-29.

11 Kong J, Zerfos P, Luo H, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks[C]//Proc. of International Conference on Network Protocols. 2001.

12 Luo H, Zerfos P, Kong J, et al. Self-securing Ad Hoc Wireless Networks[C]//Proc. of the 7th IEEE Symposium on Computers and Communications. 2002.

13 Capkun S, Hubaux J P, Buttyan L. Self-organized Public-key Management for Mobile Ad Hoc Networks[J]. IEEE Transactions on Mobile Computing, 2003, 2(1): 52-64.

14 Josang, Gray A E, Kinateder M. Semantic Constraints for Trust Transitivity[C]//Proc. of APCCM'05, Newcastle, Australia.2005-01.

15 Shamir A. Identity-based Cryptosystems and Signature Schemes[C] //Proc. of Conference on Advances in Cryptology. [S.l.]: Springer-Verlag, 1984: 47-53.

16 Khalili A, Katz J, Arbaugh W. Toward Secure Key Distribution in Truly Ad-Hoc Networks[C]//Proc. of 2003 Symposium on Applications and the Internet Workshops. IEEE Computer Society, 2003: 342-346.

17 Deng H, Mukherjee A, Agrawal D P. Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks[C]//Proc. of International Conference on Information Technology: Coding and Computing. 2004.

18 Girault M. Self-certified Public Keys[C]//Proc. of Conference on Advances in Cryptology. [S.l.]: Springer-Verlag, 1991: 490-497.

19 Van der Merwe J, Dawoud D, McDonald S. Trustworthy Key Management for Mobile Ad Hoc Networks[C]//Proceedings of South African Telecommunication Networks Architectures Conference, Stellenbosch, South Africa. 2004.

20 Arazi O, Qi H. Self-certified Group Key Generation for Ad Hoc Clusters in Wireless Sensor Networks[C]//Proc. of the 14th IEEE International Conference on Computer Communications and Networks, San Diego, CA. 2005.

21 Balfanz D, Smetters D K, Stewart P, et al. Talking to Strangers: Authentication in Ad-Hoc Wireless Networks[C]//Proceedings of Network and Distributed System Security Symposium'02. 2002.

22 Bellovin S M, Merritt M. Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks[C]//Proceedings of the 1992 IEEE Symposium on Security and Privacy. [S.l.]: IEEE Computer Society, 1992: 72-84.

23 Becker K, Willie U. Communication Complexity of Group Key Distribution[C]//Proceedings of the 5th ACM Conference on Computer and Communications Security. [S.l.]: ACM Press, 1998.

24 Asokan N, Ginzboorg P. Key Agreement in Ad Hoc Networks[J]. Computer Communications, 2000, 23(17): 1627-1637.

25 Lamport L. Password Authentication with Insecure Communication [J]. Communication of the ACM, 1981, 24(11): 770-772.

26 Perrig A, Canetti R, Tygar J, et al. Efficient Authentication and Signing of Multicast Streams over Lossy Channels[C]//Proc. of IEEE Symposium on Security and Privacy. 2000-05.

27 Perrig A, Szewcyk A, Wen V, et al. SPINS: Security Protocols for Sensor Networks[J]. Journal of Wireless Networks, 2002, 8(5): 521-534.

28 Elhdhili M E, Azzouz L B, Kamoun F. A Totally Distributed Cluster Based Key Management Model for Ad Hoc Networks[C]//Proc. of the 3th Annual Mediterranean Ad Hoc Networking Workshop. 2004.