Hans Journal of Wireless Communications 无线通信, 2011, 1, 6-10
http://dx.doi.org/10.12677/hjwc.2011.11002 Published Online August 2011 (http://www.hanspub.org/journal/hjwc/)

Researches on Trust Building Scheme Relevant Issues in Wireless Self-Organizing Network*

Haitao Wang
Institute of Communication Engineering, PLA University of Science and Technology, Nanjing
Email: haitmail@126.com
Received: Jun. 8th, 2011; revised: Jul. 21st, 2011; accepted: Aug. 1st, 2011.

Abstract: Building trust relationship in acentric and distributed wireless self-organizing network (WSON) is vital for ensuring network security, but it still faces many new problems and challenges. In this paper necessity of introducing trust schemes in WSON is introduced firstly. Then, concepts and functions of trust are expounded. Based on above elaboration, trust building methods, trust models and trust assisted secure routing schemes are explained. Finally, various attacks faced by trust building scheme and countermeasures are summed up.

Keywords: Wireless Self-Organizing Network; Trust Relationship; Trust Model; Security Routing

无线自组网中的信任建立机制相关问题研究*

王海涛
解放军理工大学通信工程学院，南京
Email: haitmail@126.com
收稿日期：2011 年 6 月 8 日；修回日期：2011 年 7 月 21 日；录用日期：2011 年 8 月 1 日

摘　要：在无中心、分布式的无线自组网中建立信任关系对于确保网络的安全性至关重要，但是面临许多新的问题和挑战。首先，介绍了在无线自组网中引入信任机制的必要性。然后，阐述了信任的概念和作用。在此基础上，说明了信任建立的方法、信任模型以及信任辅助的安全路由机制。最后，归纳了信任建立机制面临的攻击及应对措施。

关键词：无线自组网；信任关系；信任模型；安全路由

1. 引言

无线自组网(Wireless Self-organizing Network)是计算机网络和移动无线通信网络相互融合发展的产物，其显著特点是节点采用无线通信方式、网络无中心、自组织和多跳中继，Ad Hoc 网络(MANET)、无线传感网(WSN)和无线网状网(WMN)都可归属于无线自组网这一范畴[1]。安全性是关系到无线自组网能否得到广泛应用重要因素之一，特别是在军事上和商业上的应用。但是，相比于传统的有线和无线网络而言，无线自组网的安全性问题更加复杂并面临更大的困难和挑战。无线自组网不依赖固定基础设施，不存在命名服务器和目录服务器等网络设施，通常也没有可信赖的中心节点，无线自组网的网络拓扑结构、网络节点数量和运动方式及其各节点之间的信任关系都处于动态变化之中。上述特点不仅使无线自组网易受各类安全威胁和攻击，而且使得现有的许多安全机制不适合用于无线自组网。

大量事实表明，无线自组网的安全挑战很大程度上在于此类网络的正常运转依赖于分布式实体(节点)之间的协作。但是，在这类网络中节点之间的协作关系是松散和脆弱的，容易受到自私行为、恶意攻击以

*基金项目：国家自然科学基金资助项目(61072043)。

及误配置和误操作的影响，问题的本质就是节点不能确定可否信任和它进行协作的其他节点[2]。当网络节点彼此之间不能信任时，就无法保证安全可靠地交互信息和协作完成任务。一方面，如果节点轻易相信其他节点，那么更容易遭到恶意攻击；另一方面如果节点间过度怀疑而不愿合作，那么必会降低网络的效用。因此，在无线自组网中(特别是当网络节点分属多个机构时)建立、管理和评价信任关系对于网络安全路由、授权和访问控制、恶意节点检测以及激励节点间的协作而言都至关重要。但是，至今无线自组网仍没有完善的信任建立和评价体系。本文将对无线自组网中信任关系的建立方法以及可能遭受的攻击手段和防范措施进行分析和探讨。

2. 基本概念

信任是一种建立在自身知识经验和对象实体属性认识基础上的判断，是一种实体与实体之间的主观行为。早在 1996 年，M. Blaze 等人就针对开放系统提出了信任管理的概念，其基本思想是在承认开放系统中安全信息的不完整性的前提下，系统的安全决策需要依靠可信任的第三方提供附加的安全信息[3]。迄今，网络安全领域对信任还没有明确和统一的定义。绝大多数学者都认为信任是确保分布式系统安全的基本要素之一，但对于信任的本质和信任的作用仍没有达到完全共识。一种评价信任的基本思路是基于监控机制来生成描述节点的可信性、可靠性和能力的信任值，然后利用这种信任信息来辅助建立安全路由、检测恶意节点和激励节点协作。

当网络节点之间建立了信任关系之后，那么节点可以预测其他节点的行为、评判它们的安全状态和诊断它们的安全问题。概括来说，信任关系有助于解决以下安全问题[4]：

- 基于对其他节点行为的预测，节点可以避免与不信任的节点协作(如节点仅选择最可信的节点转发分组)，减少了遭受攻击的机会，从而改善了网络的安全性和健壮性；
- 对节点今后行为的预测可以确定网络面临的安全风险，然后可以基于风险程度相应调整网络操作(如风险变大时采用更强壮的安全机制)，从而提供更灵活的安全解决方案；
- 信任评价可以发现信任值较低的网络节点，进而检测和隔离行为异常的节点；
- 通过对各网络节点的可信性进行评定，可以定量评估整个网络系统的可信任程度；
- 无线自组网中，网络没有可信任的中心授权节点并且节点容易遭受各种恶意攻击，在网络节点间建立的信任关系有助于实施分布式认证和防范攻击。

3. 信任建立相关机制

3.1. 建立信任的方法

无线自组网的拓扑结构和成员处于动态变化之中，节点之间的信任关系也在不断变化，信任关系是一种动态的过程，是随着时间变化的，且具有主观性，不确定性和模糊性。因此传统网络中基于静态配置的信任建立方案在无线自组网中是不可行的。在这种网络中，个体间的信任既取决于个体之间的直接接触，也取决于其他个体的推荐，同时推荐者的可信度也决定其推荐个体的可信度。尽管在理论上可以采用集中式或分布式方法建立信任关系，无中心的无线自组网倾向采用分布式信任建立方法。为了建立信任关系，每个网络节点需要维护一个信任管理器，如图 1 所示[2]。信任管理器主要包括信任建立模块和信任记录表。信任记录表用于存储有关节点之间的信任关系及相应的信任值。在需要相互协作的节点之间建立的信任关系包括直接信任和间接信任关系，可使用集合{主体，客体，行动，数值}来表示这种信任关系，其中数值或数值范围可描述信任的程度。信任建立模块采用两种方法来建立信息关系：当主体能够直接观察客体的行

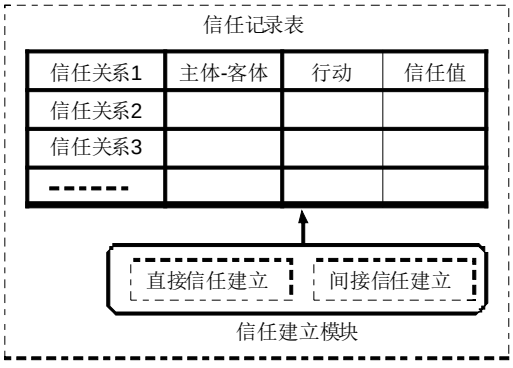

Figure 1. Components of trust manager
图 1. 信任管理器的构成

为时，可以建立直接信任；当主体从其他实体获得有关客体的相关信息时，则可以建立间接信任。实际上，网络节点之间信任关系的建立往往要同时利用直接信任建立和间接信任建立两种方法。例如，Jie Li 等人提出的客观信任管理框架(OTMF)中就提到节点对其他节点的信任程度不仅依赖于直接的观察，还依赖间接的观察信息，以此获得较为客观公正的评价[5]。

直接信任关系通常基于观察主体和客体的交互历史情况来建立。假设观察到的成功交互次数为 s，失败的交互次数为 f，那么一种简单的计算直接信任值的公式为：$s/(s+f)$。间接信任关系是基于信任可以传递这一原理建立的。例如，如果 A 和 B 建立了信任关系，同时 B 又与 C 建立了信任关系，如果 B 告知 A 它对 C 的信任程度，那么 A 可以和 C 建立间接信任关系。但是，基于信任传递方式建立的间接信任必须考虑两个关键要素[4]：一是主体何时以及从何处收集其他实体的推荐信息；二是如何根据推荐的信息来计算间接信任值。由于间接信任可能涉及一条或多条推荐路径，每条推荐路径又包含一跳或多跳。所以需要适当的信任模型来决定如何根据信任传递路径来计算间接信任值。此外，主体对客体推荐信任的判定往往通过检查观察信任和推荐信任的一致性来实现。

3.2. 信任模型

传统网络环境中的信任模型是基于认证中心(CA)的集中式信任模式。但是，这种信任模型存在可扩展性差，单点失效等问题，难以适应无线网络环境的要求。无线自组网中不能保证各个节点持有被其他节点信任的公钥，并且也无法出示可信任的证书。因此，在这种网络环境中建立分布式信任机制十分必要，这种必要性不仅体现在用户对网络的有效使用上，也体现在有利于网络的良性发展上。总的来说，信任模型可分为全局信任模型和基于局部推荐的信任模型两大类[3]。为获取全局的节点可信度，全局模型通过相邻节点间相互满意度的迭代，从而获取节点全局的可信度。基于局部推荐的信任模型在本地记录节点的历史活动信息，并询问其它节点来评价节点的可信度。局部模型通过限制反馈和评价信息范围，大大减少了获得信任所需的网络开销，易于网络规模的扩展。

另外，还可以采用一种本地组信任模型，如果一个节点对于一定数量的可信赖节点是可信的，那么认为该节点可信任[6]。但是信任关系具有时间限制(不超过证书的过期时间)。基于此信任模型，可信的节点可以为网络中的其他节点签署证书并监测其他节点的行为，如果发现行为不端的节点则撤销其证书。再有，Boudriga 提出了一种构建入侵容忍无线自组网的新方案，包含多层信任模型和一种用于资源分配和恢复的网络层机制[7]。多层信任模型假定将网络划分成两个虚拟集合：资源域和用户域。为每种活动类型分配一个唯一的信任级别，基于此信任级别和活动，用户或应用程序按照一种分布式机制分配资源，目的是最大化资源使用率和最小化成本。

需要指出的是，网络应用环境会影响要求的信任模型，进而影响密钥管理和认证的方式。举例来说，室内集会人员的移动设备构成的小型 Ad hoc 网络和战场环境中的无线传感网的信任模型就有很大不同：第一种应用情景中移动设备工作在安全和友好的环境中，移动设备之间是彼此信任协作的关系；在第二种情景中，无线设备操作在极度恶劣的非可信网络环境中，面临大量的安全威胁，节点之间的信任关系是不确定。

另外，信任模型可以用于设计适合无线自组网的分布式密钥管理方案。考虑到很多场合下无线自组网中的节点是协同工作的，一种解决密钥管理的方法是用团体用户来代替证书权威机构，密钥管理服务由一组节点协作来完成[8]。这种方法认为：无线自组网中不存在可信任的中心节点，但是一定数量的节点构成的节点组是可信任的，并且网络中一定时间内不可信的节点数量远小于可信任的节点数量。与此类似，基于 PGP(Pretty Good Privacy)的密钥管理方案中，每个节点基于 PGP 来创建它自己的公钥和私钥，并且节点自组织地存储、分发和管理证书[9]。公钥证书的发布基于节点之间现有的信任关系，并且定期在可信的节点之间发放和更新证书以防止多个攻击者发起的合谋攻击。

3.3. 信任的委托和传递

无线自组网是一个动态自组的临时网络，不能保证网络中各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，一种在网络节点之间建立信任的方法是允许在节点之间委托信任，已

建立信任关系的节点组通过向网络中其他成员传递信任关系来扩展可信任的群体规模。

在此以一个小型网络为例来说明这种信任建立方法，首先我们假设所有节点之间都存在连接，并且采用一种反应式路由协议。信任建立方法具体描述如下：如图2所示，一个小型无线自组网由3个信任组G1、G2、G3组成，假设节点A作为委托信任的代理，A通过广播一个START消息来发起信任传递过程，网络中收到此消息的每个节点向网络广播含有信任公钥的消息，于是A可以在无线自组网中建立和认证一张信任关系映射表，G2组的所有节点与A通过节点C能够建立一种间接的信任关系，A可以通过C得到G2中的签名的公钥，而G3中的节点与A没有信任关系，但是A可以与G3中的节点G手工交换信任密钥，而后通过G获得G3中的签名公钥，最后A将收集到的签名密钥在整个无线自组网中传播，最终能够使G1～G3中的每个节点之间都能建立信任关系，并且因此产生一个新的信任组G4。这种方法能够被扩展用于在任意规模的无线自组网中建立信任关系。但是，应该看到这种方法存在一定的缺陷，因为它是以信任组为单位传递信任关系的，如果一个组中的任何一个节点被攻击者俘获，而且这个被占领节点并没有被其他节点发现的话，攻击者将威胁整个无线自组网的安全。因此，为了增强安全性，每个信任组中的节点必须定期进行互相认证，这种认证的频率不需要太快，以防止过量的网络开销。此外，如果一个节点要发送机密的信息时，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。

3.4. 信任辅助的安全路由机制

在 MANET 中确保路由协议的安全至关重要，在此简要介绍一种信任辅助的安全路由查找的过程[4]：

1) 当源节点希望向目的节点传输数据时，首先要寻找到目的节点的多条路由。然后，源节点查看自己的信任记录表以了解它是否与这些路由上的节点存在信任关系。如果没有信任关系，源节点向邻居节点广播推荐信任的请求消息并等待应答；

2) 收到推荐信任的请求消息后，拥有相应信任信息的节点会予以应答，并且会检查请求消息传递的跳数是否超过预设门限：如果不超过则继续向其邻居节点转发请求消息；否则丢弃该请求消息；

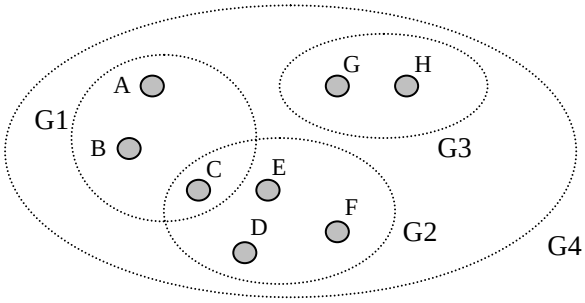

Figure 2. A small scale wireless self-organizing network consisting of three trust groups
图 2. 一个由三个信任组构成的小型无线自组网

3) 源节点收集所有的应答消息并根据信任模型计算和更新找到的路由上节点的信任值；

4) 源节点根据路由上节点的信任值计算每条路由的可信度，然后选择可信度最高的路由传输分组；

5) 在数据传输过程中，源节点可以根据需要监视路由上节点的分组转发行为；

6) 在数据传输后，源节点比较它观测到的信任值与它以前收到的推荐值。如果两者之差小于预设门限，则将推荐值标记为良好；否则将其标记为无效。然后据此更新推荐信任值；

7) 源节点更新为其转发分组的节点的直接信任值，并将信任值低于门限的节点视为恶意节点。

4. 信任关系面临的攻击和防护措施

基于信任关系可以有效检测异常行为的节点并改善网络的性能，但是也会遭受多种攻击，本节简单介绍信任建立机制面临的各种攻击和应对策略[2]。

4.1. 流言(Bad Mouthing)攻击

针对基于推荐的信任建立方法，攻击者可以提供虚假的推荐来诋毁合法节点并提升恶意节点的信任值。通过严格地构建和利用推荐信任可以防范这种流言攻击：首先，严格区分对待间接推荐信任和常规的直接信任，必须根据推荐的节点的实际行为来评判推荐信任；第二，信任传递必须满足必要的条件，例如只有当推荐的信任超过预定门限值时才允许信任传递。

4.2. On-Off 攻击

On-Off 攻击也称间歇式攻击，恶意节点交替地表

现出攻击行为和正常行为，目的是期望在不被用户发现的情况下实施攻击。这种攻击实际利用了信任的动态特性。信任是一种动态行为，合法的实体可能由于被敌方俘获而变成恶意实体，不合格的实体也可能因为环境变化而成为符合条件的实体。举例来说，在无线自组网中，一个移动节点所处的信道环境是动态变化的，只有当它所处的信道条件较好时才能够胜任转发分组的任务。基于这种考虑，应该赋予较早观察到的信任值较低的权重，并且可引入遗忘因子f(取值介于 0 和 1 之间)来描述这种特性。但是现有的信任建立机制通常使用固定的遗忘因子，这种做法不能很好地阻止攻击者发起的 On-Off 攻击。针对这一问题，可以基于人类社会中的一个社会现象来设置遗传因子，即：建立好的声誉需要长时间有好的行为表现，而破坏声誉只需要短时间内从事坏的行为。与此相对应，信任建立方法中规定恶意行为记忆的时间要长于正常行为的记忆时间。因此引入基于当前信任值的自适应遗忘因子f_a，当前节点实施正常行为的概率越大，则f_a越小。采用这种自适应遗传因子，攻击者实施 On-Off 攻击要付出更大的代价。

4.3. 冲突行为攻击

On-Off 攻击中攻击者在时间域上表现出不同的行为，而冲突行为攻击是指攻击者针对不同的用户表现出不同的行为或执行不同的操作，目的是降低某些合法用户的信任值。例如，攻击者 X 可以总是对一组节点 G1 表现出正常的行为，而对另一组节点 G2 表现出恶意行为，使得 G1 中的节点和 G2 中的节点对 X 的信任值具有截然不同的评价，进而达到降低 G1 中节点和 G2 中节点之间的信任程度的目的。为了防范这种攻击，则需要观察节点对不同节点的行为，并在怀疑出现这种攻击时不再使用基于推荐信任的恶意节点检测方法。

4.4. 女巫(Sybil)攻击和新用户攻击

恶意节点通过伪造合法用户的 ID 发起攻击，从而降低合法用户的信任值。另外，如果恶意节点能够作为新用户进行注册，那么它可以轻易清除它的不良记录，继而实施攻击，这种攻击称为新用户攻击。信任管理本身难以防范这两类攻击，但是可以借助于认证和访问控制加以防范，使攻击者难以注册一个新的或伪造一个 ID。

5. 小结

随着无线自组网研究和应用的不断深入，安全问题的重要性越来越突出。由于无线自组网本身在安全方面的弱点和应用环境的多样性，安全机制的设计和实现更加复杂和困难。本文主要分析和探讨与网络安全紧密相关的信任建立机制，介绍了信任的基本概念和内涵，说明了信任建立的方法、信任模型即信任辅助的安全路由查找过程，并归纳了信任建立机制面临的攻击及应对措施。今后，一方面要对信任评价机制及其效用进行研究，另一方面还要考虑加强信任机制的健壮性以应对多样化的攻击方式[10]。

参考文献 (References)

[1] 郑少仁, 王海涛, 赵志峰等. Ad Hoc 网络技术[M]. 北京: 人民邮电出版社, 2005.
[2] A. Josang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2005, 43(2): 618-644.
[3] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In: J. Dale, G. Dinolt, eds. Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996: 164-173.
[4] Y. Sun, Z. Han, and R. Liu. Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine, 2008, 46(4): 112-119.
[5] J. Li, R. D. Li. Future trust management framework for mobile ad hoc networks. IEEE Communications Magazine, 2008, 46(4): 108-114.
[6] H. Yang, H. Luo. Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications Magazine, 2004, 11(1): 38-47.
[7] M. Lima, A. Santos, and G. Pujolle. A survey of survivability in mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 2009, 11(1): 66-77.
[8] D. Joshi, K. Namuduri. Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: An analysis. Journal of Wireless Communications and Networking, 2005, 2005(4): 579-589.
[9] N. Boudriga, M. Obaidat. Fault and intrusion tolerance in wireless ad hoc networks. Washington: Wireless Communications and Networking Conference, 2005, 4: 2281-2286.
[10] 王良民, 郭渊博. 容忍入侵的无线传感网络模糊信任评估模型[J]. 通信学报, 2010, 31(12): 37-44.

