文章编号:1001 - 9081(2009)05 - 1308 - 04

移动 Ad Hoc 网络信任管理综述

王衡军[1],王亚弟[1],张 琦[2]
(1. 信息工程大学 电子技术学院, 郑州 450004; 2. 92117 部队, 北京 100072)
(wanghengjun@163.com)

摘 要:移动 Ad Hoc 网络是由移动节点组成的无线移动通信网络,具有动态拓扑、无线通信的特点,易受到各种安全威胁。信任管理为实体间的相互信任问题提供了决策框架,是移动 Ad Hoc 网络安全方案的基础。综合分析了移动 Ad Hoc 网络信任管理研究的最新进展。首先介绍了移动 Ad Hoc 网络中信任关系的特点及信任管理的分类,然后对每个类型的一些典型信任管理方案进行了分类论述和综合比较,最后指出了下一步研究中应当着重考虑的问题。

关键词:移动 Ad Hoc 网络; 网络安全; 信任管理
中图分类号: TP393.08 **文献标志码**:A

Survey of trust management in mobile Ad Hoc networks

WANG Heng-jun[1], WANG Ya-di[1], ZHANG Qi[2]
(1. *Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan* 450004, *China*;
2. *No.* 92117 *Army Unit of PLA, Beijing* 100072, *China*)

Abstract: Mobile Ad Hoc networks, composed of mobile wireless nodes, are particularly vulnerable due to their features of open medium and dynamically changing topology. Trust management is the scheme for building trust between nodes in mobile Ad Hoc networks and it is the security base of mobile Ad Hoc network. The state of the art in trust management of mobile Ad Hoc networks was surveyed. Firstly, the characteristics of trust relationship in mobile Ad Hoc network and different types of trust management in mobile Ad Hoc network were analyzed. Secondly, some typical trust management schemes were reviewed. A comparison and discussion of their respective merits and faults was made at the same time. Finally, the challenges worthy of further research in this area were presented.

Key words: mobile Ad Hoc network; network security; trust management

0 引言

移动 Ad Hoc 网络(Mobile Ad Hoc Network, MANET)是由一组带有无线收发装置的移动节点组成的一个无线移动通信网络,它不依赖于预设的网络基础设施而临时组建。网络中移动的节点利用自身的无线收发设备交换信息,当相互不在彼此通信范围内时,可以借助其他节点的中继来实现信息交换。由于 MANET 是一个开放、动态的多跳网络,节点可以任意加入和退出,同时网络中没有权威中心对这些节点进行管理,节点之间也没有静态稳定的信任关系,因此,对于一个节点来说无法保证其协作节点行为的可靠性。在敌对环境中,MANET 需要在节点间建立安全可信的通信环境。信任管理为节点间的相互信任问题提供了决策框架,为保密性、完整性和不可抵赖性等安全目标的实现提供了低层平台,是 MANET 安全解决方案的基础结构。

信任管理(Trust Management)这一概念是为了解决分布式环境中的信任问题首次由文献[1]提出,目的是通过授权委托的方式解决"陌生人"授权问题。

1 移动 Ad Hoc 网络中的信任管理

1.1 移动 Ad Hoc 网络中信任关系的特点

虽然 MANET 和传统网络的安全目标是一致的:可用性、机密性、完整性、认证性、不可否认性等,然而,有限的计算、有限的通信带宽和动态的网络拓扑都使得在 MANET 中建立信任关系十分困难。MANET 节点间信任关系的特点如下。

1)缺乏信任基础设施。传统网络中主机之间的连接是准静态的,具有较为稳定的拓扑,可以通过由多种安全服务构成的基础设施来为节点间的信任提供保障。这些基础设施包括证书授权机构 CA、目录服务器和密钥管理中心 KMC 等。这些基础设施一般是在线与可达的,因此,节点可以依赖于固定的信任体系结构来作出对另一节点可信任程度的判断。而 MANET 的特点决定了节点间的信息交换存在着较大的不确定性,从而影响了类似信任基础设施的作用。同时,中心服务节点的存在为敌对方的攻击提供了有效的目标,敌方对这些目标的攻击成功将会使网络安全面临严重的危机。

2)短期、快速、在线。在传统网络中,信任关系是长期而可靠的,信任决策的依据不会经常变化,因此,对节点的信任不需要频繁的重新评估。相反,MANET 内节点信任建立的依据没有长期的稳定性。在战场上,移动节点的安全性在一定程度上依靠它所在的位置,不可能提前预知。同时,如果节点被敌人俘获,来自被俘获节点的信任关系将不再有效,新的信任依据需要被重新收集和评估。因此,信任联系是短暂的,信任的评估和信任依据的收集是个周期性频繁发生的过程。而

收稿日期:2008 - 11 - 11;**修回日期**:2009 - 01 - 17。 **基金项目**:国防预研项目。

作者简介:王衡军(1973 -),男,湖南衡阳人,讲师,博士研究生,主要研究方向:信息系统安全、计算机网络安全; 王亚弟(1953 -),男,甘肃兰州人,教授,博士生导师,主要研究方向:信息系统安全、计算机网络安全; 张琦(1974 -),女,河南郑州人,工程师,硕士,主要研究方向:计算机网络。

且这一过程必须执行迅速,以避免无线通信系统固有的时延问题。MANET 中各个节点之间的信任关系及评估几乎完全依赖在线信息,因为离线的收集和评估在大多数情况下将是毫无意义的。

3)依靠不完整信任依据。传统网络中,网络的连通性是由冗余的通信链路所保证的,由于节点间连通失败而导致已建立的信任关系不可用几乎是不可能的。然而,在 MANET 中,并不是所有节点随时可达,同时,对任何节点在任何时刻建立的信任联系也不能保证可用性。因此,在 MANET 中信任关系是在信任依据不完整甚至是不确定的情况下建立的。

1.2　移动 Ad Hoc 网络中的信任管理及其分类

MANET 中的信任管理是传统信任管理结合了 MANET 特点的特例。根据信任建立方式的不同,信任管理可以分为基于策略和基于声誉的信任管理。

基于策略的信任管理中信任关系的建立是基于对方是否具有能证明自己的凭证。信任关系通过凭证或凭证链建立。这种信任管理的结论是一个非 0 即 1 的二元决策结果。文献[1]提出的 PolicyMaker 和 KeyNote 将授权与公钥绑定,互相认识的个体根据相互间信任关系直接签署授权凭证,以授权委托的方式实现信任传递,两个陌生个体之间如果存在"信任链"就可以进行授权,也可以签署间接凭证。这种信任管理系统最终体现为一个分布式授权系统。采用了类似思想的 SPKI[2]、RT[3]、dRBAC[4]等分布式授权系统中,授权个体收集被授权个体的所有相关信息(凭证),根据本地策略和授权请求通过策略推理引擎检查一致性,决定是否授权。具体到 MANET 的应用中,凭证可以是共享的口令、对称密钥、传统单 CA 证书、分布式 CA 证书、自组织 CA 证书等。

基于声誉的信任管理参考了人类社会中信任建立的过程,信任关系根据主体以往的特定行为来建立。这种信任管理中,客体通过对主体以往行为的分析作出其未来能提供某服务的可能性的判断。MANET 中,主体以往的行为一般是节点在网络路由协作和安全协作中的特定表现,如包的转发率、证书服务的正确率等。

不同的文献给出了不同的分类方法。常见的与基于策略和基于声誉分类方法类似的信任管理分类方法还有基于凭证和基于证据的、基于身份和基于行为的、理性和感性的、客观和主观的等信任管理分类方法。这些分类方法的含义基本相似。本文中的声誉与不同文献中的信任值、信任度、可信度等词有相同或类似的含义。

2　基于策略的信任管理

目前,MANET 中主要有以下几种基于策略的信任管理方式。

2.1　传统可信第三方信任模型

传统可信第三方信任模型中,凭证可能是由可信任的第三方发布的全网或某区域共享的口令或对称密钥,也可能是由可信第三方签发的证书。这种方式存在着单点失效的问题,但是由于其简单高效的特点,在较小的区域和特定方案中也得到了较多的应用。

文献[5]的基于多级簇的信任方案使用对称密钥体制。同等级的簇组成一个层,所有的层组成一个等级体系,密钥的产生、分配以及实际的传递沿着体系进行。每一层有一个层密钥,由密钥服务器按需产生,为本层所有成员所知;每个簇有一个簇密钥,由簇首产生,为本簇所有成员的所知。簇首与簇内每个节点都有一个共享密钥。簇之间有一个簇共享密钥,用于不同簇之间的节点协商会话密钥。各种级别的密钥和分层体系提供了对选择性通信机制的支持。当有节点加入或离开时,簇必须更新簇密钥。该方案具有扩展性、高效性,但安全性较低,存在着单点失效的问题。文献[6]同样采用了共享的对称密钥来实现 MANET 中簇内的信任。文献[7]采用了由簇首充当的 CA 节点来颁发证书而实现簇内节点信任的方式。

2.2　局部分布式信任模型

局部分布式信任模型对传统可信第三方信任模型进行扩展,认为单个节点不值得完全信赖,而一个选定节点的集合则是可依赖的。该模型基于 Shamir 的 (k,n) 门限机制[8],将对单个节点的信任分散为对一组节点的共同信任,由这一组节点各自分担一部分信任,共同承担单个可信第三方的全部职责。其基本思想是:将秘密 S 分成 n 份(每份称为秘密分量或影子),n 个被选定的特殊节点掌握其中的一份。任意大于或等于 k 个特殊节点合作就可以恢复秘密 S,而小于 k 个的特殊节点则无法得到关于 S 的任何信息。文献[9]基于该思想而首先提出了部分分布式 CA 模型。文献[6]认为由簇首组成的网络范围较大,为了保证安全而采用了局部分布式信任模型。同样地,文献[10]在异构节点间也采用部分分布式 CA。

2.3　完全分布式信任模型

完全分布式信任模型最早由文献[11]提出,与局部分布式信任模型不同的是,此模型将一个 RSA 证书签名密钥分量分发给网络中所有节点。这样,在有新节点要求加入时,网络中任意 k 个节点就可以合作为新节点生成新的私钥共享分量。这类模型比局部分布式信任模型的可用性得到了提高,但是,由于密钥分量更为扩散,其安全性则有所降低。

2.4　基于身份的分布式信任模型

文献[12]提出了一种基于身份标识的加密和签名方案,该方案用主体的易识别且唯一的特征比,如姓名或 email 地址作为公钥和证书,所以,在认证之前不需要交换公钥。但是,在系统初始化的时候需要一个 CA 来产生主体的私钥。该方案中,私钥的产生与分发过程中的安全问题是关键。具体到 MANET 应用中,为了使私钥在产生时不为其他节点所知,一般也采用秘密共享的思想由多个节点组成分布式 CA,由门限个 CA 节点联合产生节点的私钥。这些 CA 节点各自产生私钥的一部分而不能得到全部私钥。文献[13-16]对该类方案在 MANET 中的应用作了具体的研究。

2.5　完全自组织的信任模型

文献[17]提出了一种完全自组织的信任方案,在这种方案中,不需要任何集中式的认证中心,将公钥的管理完全分布到各节点上,每个节点自行完成证书的签发、更新等工作。每一个节点都是一个 CA,可以给其他节点颁发证书。如果一个节点 u 想要认证节点 v,就合并它们的本地证书库,以找到一个从 u 到 v 到证书链。该文献提出了几种用户证书数据库的构成算法并分析了它们各自在信任管理中表现出的性能。文

献[7]所依赖的信任方案也是基于完全自组织信任模型构建。文献[18-19]分别引入了信任图和双向信任模型来建立完全自组织的信任模型。

2.6 移动 Ad Hoc 网络中基于策略的信任模型的比较

移动 Ad Hoc 网络中基于策略的信任模型的比较如表1所示。

表1 移动 Ad Hoc 网络中基于策略的信任模型比较

模型	基础结构	凭证	信任确认	优势	劣势
传统可信第三方模型	全网或子网(簇)设立一个可信节点	由该节点发布的签名证书或对称密钥	通过系统公钥或自己掌握的同一对称密钥验证	简单、高效	存在单点失效问题,安全性不高,不适合大范围使用
局部和全部分布式模型	系统私钥分成若干份由不同节点共享,公钥由所有节点所知	由门限个 CA 节点联合颁发	系统公钥验证	防止单点失效,验证快速、简单,适合战场等紧急场合使用	消耗较多节点和网络资源
基于身份的分布式模型	系统私钥分成若干份由不同节点共享	根据对方节点 ID 计算而得	无需确认,非法节点无法解密消息	使用简单、快速,能防止单点失效	私钥的产生与分发过程存在较大安全风险
完全自组织模型	各节点的公钥通过交换,形成本地证书数据库	节点自己生成,通过信任节点间的传递来分发	合并证书库形成证书链认证	防止单点失效,无需权威机构参与,适合自主性强、安全需求低等场合	认证链中节点的可信性难以保证

3 基于声誉的信任管理

基于声誉的信任管理的本质就是通过综合分析直接交互经验和其他节点推荐的间接经验,以评估对特定节点的信任程度,并使信任评估结果能正确地体现节点未来的实际行为。典型的,信任度随着节点行为和时间而改变,行为好的节点的信任度增加或保持不变,具有不良行为的节点的信任度相应降低,而来自不同节点的经验在信任评估所占的权重则随着时间增加而降低。一旦节点被认定为恶意节点,它将遭到全体网络成员的排斥。

MANET 中基于声誉的信任管理有两个关键的环节:行为监视和声誉评价。

3.1 基于声誉的信任管理中的行为监视

行为监视是信任管理的第一步,节点通过相互监视来得到邻居节点的第一手资料,是后续声誉评价的基础。文献[20]提出了一种名为 watchdog 的监视方法,watchdog 运行于每个节点上,负责监视邻居节点的行为。通过本地监视技术来发现和排除不良节点的思想在很多研究[21-22]中都得到了普遍的应用。文献[7]采用了分层监视的方法,全网节点按信任值划分为五个等级,高等级的节点监视低等级的节点的行为,只有最高等级的节点才有可能担任 CA 和簇首。

除了普遍应用的本地监视技术外,还可以通过信任推荐的过程来判定不良行为。如当采用完全自组织信任方案时,当节点需要远程节点的证书时,它可以向多个中间节点要求推荐该远程节点的证书,通过对比来自不同节点推荐的该远程节点的证书,可以发现其中的恶意推荐行为[23]。

3.2 基于声誉的信任管理中的声誉评价

声誉评价是基于声誉的信任管理的核心问题,其依据是自身通过本地行为监视得到的直接经验和其他节点推荐的间接经验。目前出现了不少的评价方案,部分声誉评价方案在一些 MANET 的信任管理方案中得到了应用。本文中的声誉评价与不同文献中的信任评估、信任评价、信任计算、信任合成等词有相同的含义。

1)基于权重的声誉评价方案。文献[24]提出了基于权重的声誉评价方案,对不同推荐路径的推荐信任值进行加权平均。权重由来源节点的信誉、声誉产生的时间等因素决定。这种方法简单直观、易于理解,然而,不满足声誉评价的结合率,相同的信任证据通过不同方式评价,会产生不同的结果。并且该模型中的推荐权重参数主观性非常强,在移动 Ad Hoc 网络环境中难以确定。

2)基于概率的声誉评价方案。文献[25]首先引入了经验的概念来表述和度量声誉,并给出了由经验推荐所引出的声誉评价和综合计算公式。Beth 模型的声誉综合计算采用简单的算术平均,无法很好地消除恶意推荐所带来的影响[26]。文献[23, 27]采用了与 Beth 方法类似的声誉评价方法。文献[28-29]将实体间的信任关系分为直接信任值和信任强度,提出了较为完善的基于推荐信任向量和 Beta 分布的声誉评价模型。信任论中熵的有关概念也被用于声誉评价[30]。基于概率的声誉评价方案是采用最多的声誉评价方案。

4 两者结合的信任管理

基于策略的信任管理给出的结论非0即1,过于“刚硬”,不完全适合 MANET 的动态演化过程。而基于声誉的信任管理建立较慢,易受恶意节点的干扰。因此,很多文献提出了两者结合的方案。文献[7]将传统可信第三方的信任模型与声誉评价相结合,簇首由声誉高的节点担任。同时簇首还担任 CA 的功能,负责为其他节点颁发证书,节点间的信任体现在证书链上。本地监视为声誉的调整提供依据,声誉的变化直接影响其扮演的簇内角色。文献[23]将完全自组织的信任模型与基于概率的声誉评价方案相结合,凭证链形成时不仅传递凭证而且传递节点的声誉。如果声誉过低,节点就被认为是不安全的,即使能建立证书链也不能被信任。

5 结语

目前,对基于策略的信任管理研究较多较深入,它是大多 MANET 安全应用与服务方案的基础。基于声誉的信任管理更易受到恶意节点的干扰,因此,虽然它更能体现网络运行的状况但是一般不能单独用于安全保障。本文对两种信任管理的相关研究成果进行了分析与比较。

整体来说,MANET 安全研究仍然处于理论探索阶段,其信任管理的进一步研究应考虑以下方面:资源有限的矛盾近期难以缓解,而现在的方案大多为了追求安全而较复杂,对网络和节点资源消耗大,因此,发展快速、轻型、安全、适合特定场合的信任管理方案应是具体应用面临的重要任务;现有的

声誉评价方案仍非完全合理地评价节点的各种行为,因此,继续探索新的适合 MANET 的声誉评价方案也是研究重点之一。

参考文献:

[1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management [C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society Press, 1996: 164 - 173.

[2] ELLISON C M, FRANZ B, RIVEST R, *et al.* Simple public key infrastructure certificate theory[S]. IETF RFC, 1999.

[3] LI N G, MITCHELL J C. RT: A role-based trust-management framework [C]// The 3rd DARPA Information Survivability Conference and Exposition: DISCEX Ⅲ. Washington, DC: IEEE Computer Society Press, 2003: 201 - 212.

[4] FREUDENTHAL E, PESIN T, PORT L, *et al.* dRBAC: Distributed role-based access control for dynamic coalition environments, TR2001-819[R]. New York: New York University, 2001.

[5] LI J H, LEVY R, YU M, *et al.* A scalable key management and clustering scheme for Ad Hoc networks [C]// Proceedings of the 1st International Conference on Scalable Information Systems. New York: ACM Press, 2006: 1 - 10.

[6] BECHLER M, HOF H-J, KRAFT D, *et al.* A cluster-based security architecture for Ad Hoc networks [C]// Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies: IEEE INFOCOM 2004. Piscataway, NJ, USA: IEEE Press, 2004, 4: 2393 - 2403.

[7] RACHEDI A, BENSLIMANE A. Trust and mobility-based clustering algorithm for secure mobile Ad Hoc networks [C]// 2nd International Conference on Systems and Networks Communications: ICSNC 2006. Piscataway, NJ, USA: IEEE Computer Society, 2006: 72.

[8] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612 - 613.

[9] LIDONG Z, HAAS Z J. Securing Ad Hoc networks[J]. IEEE Network Magazine. 1999, 13(6): 24 - 30.

[10] YI S, KRAVETS R. Key management for heterogeneous Ad Hoc wireless networks [C]// Proceedings of the 10th IEEE International Conference on Network Protocols: ICSNC 2006. Washington, DC: IEEE Computer Society, 2002: 202 - 205.

[11] KONG JIE-JUN, PETROS Z, LUO HAI-YUN, *et al.* Providing robust and ubiquitous security support for mobile Ad-Hoc networks [C]// Proceedings of the Ninth International Conference on Network Protocols: ICNP 2001. Washington, DC: IEEE Computer Society, 2001: 251.

[12] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. Berlin: Springer-Verlag, 1985: 47 - 53.

[13] KHALILI A, KATZ J, ARBAUGH W A. Toward secure key distribution in truly Ad-Hoc networks [C]// Proceedings of the 2003 Symposium on Applications and the Internet Workshops: SAINT'03 Workshops. Washington, DC: IEEE Computer Society, 2003: 342 - 346.

[14] 崔国华, 金豪. 基于 IBE 和秘密共享的分布式密钥管理和认证[J]. 信息安全与通信保密, 2005(2): 53 - 55.

[15] 刘波, 李之棠. Ad Hoc 网络中密钥分发机制的研究[J]. 华中科技大学学报: 自然科学版, 2003, 31(234): 244.

[16] HOEPER K, GONG G. Bootstrapping security in mobile Ad Hoc networks using identity-based schemes with key revocation, CACR 2006-04 [R/OL]. Waterloo, ON, Canada: University of Waterloo, 2006 [2008 - 09 - 06]. http://www.cacr.math.uwaterloo.ca/techreports/2006/cacr2006-04.pdf

[17] CAPKUN S, BUTTYAN L, HUBAUX J P. Self-organized public-key management for mobile Ad Hoc networks[J]. IEEE Transactions on Mobile Computing. 2003, 2(1): 52 - 64.

[18] HUBAUX J-P, BUTTYÁN L, CAPKUN S. The quest for security in mobile Ad Hoc networks [C]// Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing: MobiHoc 2001. New York: ACM Press, 2001: 146 - 155.

[19] FU CAI, HONG FAN, LI RUI-XIAN, *et al.* Self-organized public-key management for mobile Ad Hoc networks based on a bidirectional trust model [J]. Wuhan University Journals of Natural Sciences, 2006, 11(1): 188 - 192.

[20] MARTI S, GIULI T J, LAI K, *et al.* Mitigating routing misbehavior in mobile Ad Hoc networks[C]// Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. New York: ACM Press, 2000: 255 - 265.

[21] YANG HAO, SHU J, MENG XIAOQIAO, *et al.* SCAN: Self-organized network-layer security in mobile Ad Hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 261 - 273.

[22] MICHIARDI P, MOLVA R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile Ad Hoc networks [C]// Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security. Netherlands: Kluwer, 2002: 107 - 121.

[23] NGAI E C H, LYU M R. An authentication service based on trust and clustering in wireless Ad Hoc networks: Description and security evaluation [C]// Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing: SUTC' 06. Washinton, DC: IEEE Computer Society, 2006: 94 - 101.

[24] GUHA R, KUMAR R, RAGHAVAN P, *et al.* Propagation of trust and distrust [C]// Proceedings of the 13th International Conference on World Wide Web. New York: ACM Press, 2004: 403 - 412.

[25] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks [C]// Proceedings of the Third European Symposium on Research in Computer Security, LNCS 875. Berlin: Springer-Verlag, 1994: 3 - 18.

[26] 张仕斌, 何大可, 盛志伟. 信任管理模型的研究与进展[J]. 计算机应用研究, 2006, 23(7): 18 - 22.

[27] NGAI E C H, LYU M R. Trust- and clustering-based authentication services in mobile Ad Hoc networks [C]// Proceedings of the 24th International Conference on Distributed Computing Systems Workshops: ICDCSW'04. Washington, DC: IEEE Computer Society, 2004: 582 - 587.

[28] 刘玉龙, 曹元大. 分布网络环境主观信任模型研究[J]. 北京理工大学学报, 2005, 25(6): 504 - 508.

[29] 刘玉龙, 曹元大, 李剑. 一种新型推荐信任模型[J]. 计算机工程与应用, 2004, 40(29): 47 - 49.

[30] SUN YAN, YU WEI, ZHU HAN, *et al.* Trust modeling and evaluation in Ad Hoc networks[C]// IEEE Global Telecommunications Conference: GLOBECOM'05. Washington, DC: IEEE Press, 2005, 3: 1862 - 1867.