文章编号:1000-582X(2011)08-134-05

社区模型的移动 Ad hoc 网络信任管理方案

汪张生

(安徽医科大学 计算中心 合肥 230032)

摘 要:分析了移动自组网面临的安全问题,特别是由网络内部恶意结点引起的威胁。通过跟踪结点的行为,对结点的信任度进行计算和管理;可以有效限制恶意节点行为,增强网络安全性和可靠性。根据 Ad hoc 网络的特点,在所提出的方案中对信任概念的内容进行了扩展,通过网络社区模型,建立了对结点进行信任计算的公式和管理方案。仿真实验证实了该方案相对于传统方案具有更高的效能。

关键词:自组网络;网络安全;信任管理;信任辅助规则;社区模型

中图分类号:TP393.08 **文献标志码**:A

Trust management scheme based on community model for mobile Ad hoc networks

WANG Zhang-sheng

(Computer Center, Medical University of Anhui, Hefei 230032, P. R. China)

Abstract: The security issues in mobile Ad hoc network, especially caused by inner malicious nodes are analyzed. By tracking the behavior of nodes, trust level of each node can be evaluated and managed; then actions of malicious nodes will be constrained and the security and reliability of entire network are enhanced. According to the features of Ad hoc. The scheme proposed in not only extends the conception of trust but also include the trust computation model and trust management mechanism. Simulation experiments show the novel scheme is more efficient than other trust schemes in traditional protocols.

Key words: Ad hoc; network security; trust management; trust assistant policy; community model

由于移动 Ad hoc 网络不要基础设施建设,在商业和军事领域特别是在敌对环境或由于建设基础设施成本太高,网络只需短期使用等情形下,获得了越来越多的应用。然而由于 Ad hoc 网络中结点能源有限,结点的移动性,信号的传输方式及传输距离限制等方面的原因带来了很多安全和效率方面的问题[1]。

Ad hoc 网络中 2 个结点之间既可能直接通信也可能需要其他结点作为路由器进行转发,显然由于 1 个结点能够访问其他结点的资源,结点之间信任度的评价就相对重要。信任评价系统通过收集、计算、共享来完成网络的信任管理工作。在 Ad hoc 网络中,这样的机制不仅仅用于跟踪结点的行为从而检测出网络中的恶意结点,而且也用于在建立网络路由时排除行为异常的结点,使用值得信任的结点,从而加强整个网络的安全。当前的信任管理方案主要可以分为 2 类,一类是用授权委托的方式解决"陌生人"授权问题,如 SPKI、RT、DRBAC[2] 都采用这一思想。在这种信任管理系统中,信任通过凭证中的授权策略间接体现,信任不能被直接而精确的表达。另一类主要的信任管理系统,对"信任"进

收稿日期:2011-02-10

基金项目:安徽省高校基金项目(2010sk155)

作者简介:汪张生(1976-),男,主要从事移动网络安全方向研究,(Tel)0551-5161193;(E-mail)737624936@qq.com。

行量化评估,个体将所有相关信息量化,包括对被评估个体的行为观察、与被评估个体的交互记录以及其他个体的意见等,利用适当的计算模型得到对方的信任值.用信任值可以灵活地调节网络安全措施的实施,包括密码算法强度、授权决策等,使之针对不同个体进行个性化管理.

目前对 Ad hoc 网络的信任管理系统的研究主要集中于对节点进行信任值评估,借助信任值评估增强 Ad hoc 网络的安全性、健壮性等方面。

针对移动无线网络结点的处理能力低和能源限制,在提出的信任管理方案中,对传统信任概念进行了更新,把社区概念应用到网络管理中,该方案提出了一种新的信任计算模型,能够高效地计算出每个结点的信任值,而且包含能对信任系统进行全方位管理的机制;在这个分布式模型中,每个结点都可以对其感兴趣的结点进行信任评估。该方案可应用于网络管理的多个环节,例如在路由建立过程中,每一跳都可以选择最可靠的结点,保证路由安全;同样在多播应用中,可以根据信任度选择合适的邻居传递消息。

1　新的信任模型和信任管理

在 Ad hoc 这样一种开放、共享的无线网络环境中,有可能存在某些恶意的结点危害整个网络。目前,大量的研究致力于信任和名誉系统来解决这样安全问题,如 Baras[3] 等人应用随机图形理论和协作游戏理论建立了基于本地互动的信任计算模型;Boukerche[4] 等建立了一种信任管理系统,在该系统中只有可信的中间结点才能参与构建路由。通过对以往方案的分析,为了更有效的进行信任计算和管理,提出的基于信任的社区模型能够对结点的活动进行分布式评估,通过对结点信任评价能够检测和排除恶意结点,对结点进行动态管理,从而提高整个网络的安全性和可靠性。

1.1　信任和信任管理

信任是 2 个实体间的一种关系,其中一个实体相信、期望或接受另一个实体将以合适的方式操作。对信任概念进行如下扩展:信任(T)代表着在和某个结点交互时其可信、安全及可靠的程度,由 1 个连续的实数表示。不同的结点对同 1 个结点进行信任评估时的信任值可能是不一样的,只有相互可信的结点才能进行通信,结点在参与某个活动时,所有参与者都要满足发起结点的信任需求。

信任被描述为 2 个结点间为了某个特定的目的或活动建立起来的双方的一种关系[5],$T(i,j)$表示结点 I 和结点 J 的信任关系。在本方案中,任何一个结点(I)都可以容易地建立对其他结点(J)的信任评价,以判断(J)是否可以加入由(I)发起的活动。

结点的行为将作为对结点信任评价的依据,好的行为将导致信任度[6]的增加,恶意的行为将会降低对其信任度的评价,如果 J 成功的为 I 转发了 1 个数据包,结点 I 认为 J 是一个诚实结点,$T(i,j)$将会增加;如果 J 故意丢弃数据包或者在路由构建过程中有撒谎的行为,将会被相应地减少 $T(i,j)$。

1.2　社区模型

很多方案中,网络按照一定的规则被划分为若干簇[7],但簇相对来说比较复杂和难于管理,本文方案中提出了 1 个社区概念,每个结点以自身为中心,和所有直接邻居形成 1 个社区,其中可能包含有恶意结点。社区模型和 SDAR[8] 协议中组的概念相似但又有重大区别,SDAR 组中的结点按照信任程度被划分为高、中、低 3 个等级,在社区中的结点并不划分等级但拥有更多的管理机制。在社区模型中设计有 1 个特别的信任辅助规则,社区中具有最高信任值 T 的结点被指定为中心结点的辅助中心结点来完成对某个结点的信任评估。

相对于传统的信任管理方案,新方案中每个结点都有 1 个以自身为中心的社区,中心结点和邻居结点的认证通过加密技术进行[9],当 1 个新的结点加入社区时,新结点向中心结点发送其公开密钥,中心结点为其初始化 1 个信任值(T),并以初始信任值为基础产生相应的秘密密钥,该密钥将以新结点的公开密钥加密发送。结点信任值不同,所产生的秘密密钥也不同,但相同信任值的结点共享同样的秘密密钥[10]。

图 1 是以结点 C 为中心结点形成的 1 个社区,C 有 6 个邻居结点,D 和 G 为恶意结点,它们被排除在社区活动之外。

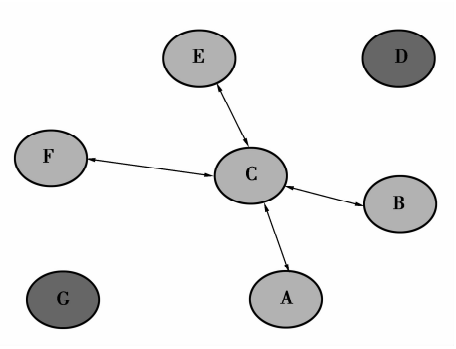

图1 以结点C为中心的社区

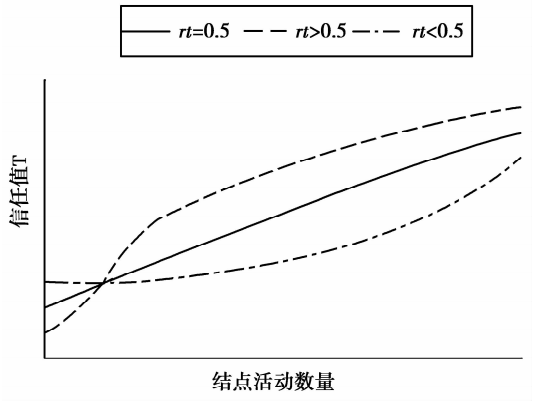

图2 结点信任值增长曲线

1.3 信任计算

在大多数的信任计算模型[11]中,信任值的计算是一个线型函数,而在本方案中,信任值是结点在社区中时间(time)和最近的信任值(rt)的函数,如果一个结点在一个社区中时间越长,那么它的可信度就应该越高,如果是一个恶意结点,按照规则它应该被检测出来并被排除在外,时间的单位为ms。另外一个参数 rt 反映的是一个结点最近的行为,如果结点参与的活动(例如构建路由,转发数据包等)多,那么 rt 将会增加,如果结点参与活动少或有恶意的行为,rt 将增加缓慢或被减少。

首先,做如下定义

$$N = 0.51 + rt, \tag{1}$$

其中0.51是一个经验数据,由系统设计人员确定,如果 N 小于1表示该结点最近的信任度低($rt<0.5$),N 大于1表示结点的最近信任度高

$$W = k^{\text{time}} \times ra, \tag{2}$$

其中:k 为折现因子,取0到1之间的值;ra 是1个结点最近的活动,可能包含有成功的转发数据,也可能包含恶意的行为。信任值T表示为公式3

$$T = \alpha \times \frac{1 - N^{(1+W)}}{1 - N}, \tag{3}$$

α 是一个比例系统,使得 T 的取值在0和1之间,每个节点可以独立的选择 k 和 α 的值,通常来说它们都是经验数据,由系统设计人员来选取。在这个方案中信任值的增长呈现3种形态[12],增长的速度取决于过去的信任值及节点在社区中的时间。图2表示了信任值 T 的增长曲线,如果节点过去的信任记录(rt)高则信任值增长较快,反之较慢。

在新的信任管理方案中采用类似与AODV[13]路由协议的方法来维持社区,中心节点周期性广播HELLO消息,在HELLO消息中包含有最新的节点信任值;同时中心节点清除变量time和 ra 的值,并用每个节点当前得信任值T赋给变量 rt。这样能对每个邻居节点进行周期性评估。

1.4 信任辅助规则

本方案采用了1个新的技术就是信任辅助规则,这也是不同于其他传统方案的地方[14]。中心节点的所有具有最高信任值的邻居节点被指定为辅助节点,它们帮助中心节点计算其他节点的信任值。当中心节点I在计算对节点J的信任值时,所有的辅助节点会把在各自社区中节点J的信任值发送给中心节点I。中心节点I把从辅助节点收到的信任值和自己按照公式3计算出来的值的平均数作为该节点的最终信任值(T_f),并以此做出相应的决定比如是否让该节点继续留在社区中。T_f 的计算如公式4所示

$$T_f = \frac{T_{(I,J)} + (T_{(A1,J)} + T_{(A2,J)} + \ldots T_{(An,J)})}{n+1}, \tag{4}$$

$T_{(I,J)}$ 表示中心节点I按照公式3计算出来的信任值T,$T_{(An,J)}$ 表示节点J在各辅助节点社区中的信任值。采用这样的计算方式能够避免某个中心节点就是潜在的攻击者或恶意节点,这样中心节点可以获得邻居节点更加可靠和客观的信任值。

2 仿真实验及性能评估

为了更好地对新方案进行分析和性能评估,使

用 NS-2 进行了仿真实验,并和一种线型信任方案进行对比。

2.1　实验场景和对比线性信任方案

实验中结点之间的联系是双向的,每个结点具有足够的运算能力完成相关操作,结点可以在 670 m×670 m 的平面上按照随机运动模式[11]运动,结点发射信号半径为 250 m。其中包含有部分恶意结点比如不参与路由构建和不转发其他结点数据。结点之间的认证采用了 RSA 算法,秘密密钥的长度为 64 位,每个实验运行的时间为 600 s。

目前大多数已被采用的信任方案普遍采用线性函数或者概率统计[15]的方法来计算结点的信任值。公式 $T=\alpha \cdot x+T_0$ 是一种典型的线性信任计算方法,x 表示一个结点的活动,T_0 表示以前信任值,这样的信任方案往往按照结点的信任值进行分组管理。

2.2　仿真结果分析

在实验过程中,选择了路由开销、发包率(实际发送的包和计划发送的包的比率)、安全开销及网络连通性等方面对新方案和线性方案做了对比[16]。

图 3 和图 4 反映了网络中恶意结点数对路由开销和安全开销方面的影响,从中可以看出,恶意结点的增加对 2 种方案中路由开销的影响都不大,新的方案在路由开销方面要小于线性方案;而恶意结点的增加对安全开销方面的影响较为明显,新的方案由于对发现的恶意结点处理较多比如将结点排除社区或取消其参与某些活动的权力等,而线性方案仅仅是对恶意结点划分不同的等级,所以在安全开销方面要高于线性方案。

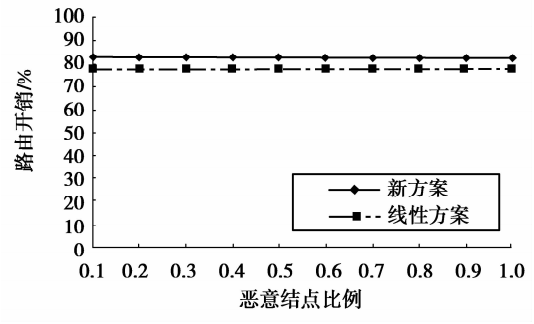

图 3　恶意结点对路由开销的影响

图 5 和图 6 反映了两种信任方案下结点移动速度对发包率和网络连通性方面的影响,结点移动速度提高,网络的发包率都会明显下降,但在这 2 个方面新方案都要优于线性方案,因为在新方案中,恶意结点会被排除在网络的通信过程中。

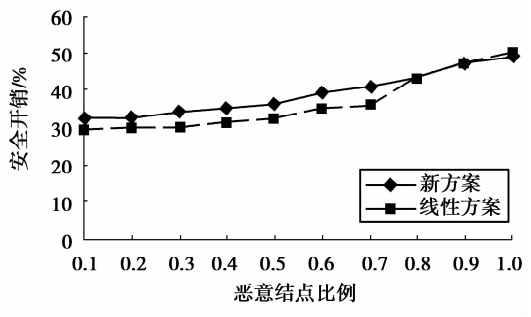

图 4　恶意结点对安全开销的影响

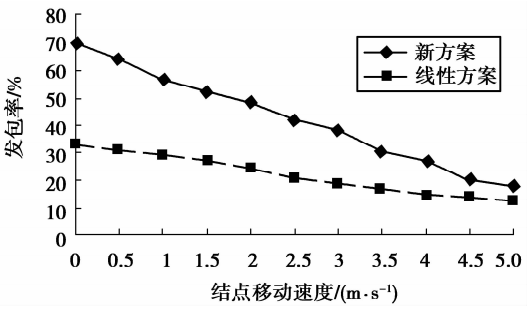

图 5　结点移动速度对发包率的影响

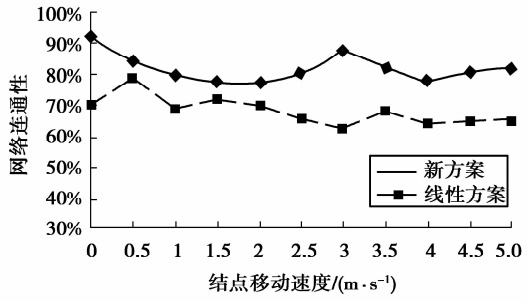

图 6　结点移动速度对网络连通性的影响

3　结　语

移动 Ad hoc 网络中信任管理问题由于其重要性和复杂性,已经成为 1 个重要的研究课题,提出的信任计算及管理模型能以一种分布、动态、高效的方式管理整个网络中的结点,仿真实验说明相当于传

统方案,该方案更为高效和简单,能够有效提高网络的安全性和可靠性。

参考文献:

[1] 郑少仁,王海涛等. Ad Hoc 网络技术[M]. 北京:人民邮电出版社,2005.

[2] ZHOU L, HAAS Z J. Securing Ad hoc networks[J]. IEEE Networks,1999,13(6):24-30.

[3] BARAS J S, JIANG T. Cooperative games, phase transitions on graphs and distributed trust in MANET [J]. Proceedings of 43rd IEEE Conference on Decision and Control, 2004:93-98.

[4] BOUKERCHE, El-KHATIB K, XU L et al. Performance evaluation of an anonymity providing protocol for wireless ad hoc networks[J]. Performance Evaluation, 2006:1094-1109.

[5] GUHA R,KUKMAR R,RAGHAVAN P. Propagation of trust and distrust[M]. New York, USA:[s. n.], 2004,17-22.

[6] LIU J, SACCHETTI D, SAILHAN F. Group management for mobile ad hoc networks: design, implementation and experiment[J]. Proceedings of the 6th conference on MDM, 2005: 47-54.

[7] BOUKERCHE A, REN Y. A novel solution based on mobile agent for anonymity in wireless and mobile ad hoc networks[J]. Proceedings of 3rd ACM workshop on Q2SWinet, 2007:86-94.

[8] ZHANG Y, LOU W, LIU W, et al. Securing mobile ad hoc networks with certificateless public Keys[J]. IEEE Transactions on Dependable and Secure Computing, 2006,3:386-399.

[9] ASOKAN N, GINZBOORG P. Key agreement in Ad hoc networks [J]. Computer Communications, 2000, 23(17): 1627-1637.

[10] 窦文. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报,2004,15(4):571-583.
DOU WEN. A recommendation-based Peer-to-Peer trust model[J]. Journal of Software, 2004, 15(4): 571-583

[11] PERKINS C E, ROYER M E, Ad hoc on demand distance vector (AODV) routing[J]. IETF Internet Draft,1997:38-40.

[12] TILMANN G, ADRIAN E. Strictly proper scoring rules, prediction and estimation[J]. Journal of the American Statistical Association, 2007, 102(477): 359-378.

[13] CARRUTHERS R, NIKOLAIDIS L. Certain limitations of reputation based schemes in mobile environments [J]. Proceedings of the 8th ACM International Symposium on MSWiM, 2005,2-11.

[14] SEN J, CHOWDHURY P R, SENGUPTA I. A distributed trust establishment scheme for mobile ad hoc networks[J]. Proceedings of Int'l Conf. on Computing: Theory and Applications, 2007,51-58.

[15] NIELSEN M, KRUKOW K, SASSONE V. A bayesian model for event-based trust[J]. Electronic Notes in Theoretical Computer Science, 2007,172:499-521.

[16] SUN Y, YU W, ZHU H, et al. Trust modeling and evaluation in Ad Imc networks[J]. IEEE Globecom, 2005:28-32.

(编辑 侯 湘)