移动 Ad hoc 网络中一种信任评估模型*)

洪 亮[1] 洪 帆[1] 张明猛[2] 余院兰[1]

(华中科技大学计算机科学与技术系 武汉 430074)[1] (江南计算技术研究所 无锡 214083)[2]

摘 要 移动 Ad hoc 网络没有固定的网络基础设施、网络拓扑结构频繁动态变化、无线信道完全开放、网络缺乏自稳定性。在这样的网络中,节点之间的相互信任对网络的安全保障与可靠运行均具有重要的意义。本文提出一个模型,用于网络节点之间的信任评估。在这个模型中,信任被定义成信任评估主体对客体的一个多角度的动态的评价,同时模型提供了一个合理的方法用于综合直接经验和间接经验。最后,将模型应用于移动 Ad hoc 的一种路由协议中,以示举例。

关键词 移动 Ad hoc 网络,信任评估,安全保障,路由协议

A Trust Valuation Model in Mobile Ad hoc Networks

HONG Liang[1] HONG Fan[1] ZHANG Ming-Meng[2] YU Yuan-Lan[1]

(Department of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)[1]

(Jiangnan Institute of Computer Technology, Wuxi 214083)[2]

Abstract Because of self-organization, dynamic topology and openness of wireless links, trust is an important thing for security and reliability of Mobile Ad hoc Network's nodes. Then a trust valuation model is given to value trust relationships between nodes. In this model trust is defined as a multiple dynamic evaluation on the object, and a reasonable method is provided to combine the direct experience and the indirect experience. As example we apply the model in a routing protocol.

Keywords Mobile Ad hoc networks, Trust evaluation, Security & reliability, Routing protocols

1 引言

移动 Ad hoc 网络是一种临时自治的分布式系统,具有无中心、自组织、节点资源有限、动态拓扑结构变化频繁等特征。移动 Ad hoc 网络不依赖于固定主干网(但可以与其配合)或基站便能够快速部署到位,建立起一套完整、强大、高抗毁的网络通信系统,提供有效的数据和多媒体通信服务。节点之间的数据通讯是通过中间节点的中继来完成的,故移动 Ad hoc 网络又称为多跳无线通讯网络。移动 Ad hoc 网络多用于军事环境、应急系统以及一些商用、家用环境中。

由于没有固定的网络基础设施、网络拓扑结构频繁动态变化、无线信道完全开放、网络缺乏自稳定性等原因,移动 Ad hoc 网络相对于有线网更易遭受各种攻击。

为了更好地解决行为异常节点对网络的干扰,特别是针对节点的自私和不合作等异常行为,在一些文献[1~5]中把信任评估机制引入到移动 Ad hoc 网络中来,其作用有 3 个:

①对节点进行信任评估,以区分可信任节点和不可信任节点;

②引导和鼓励节点执行正常操作,避免自私行为;

③将行为异常节点(包括恶意节点、不合作节点等等)从网络中孤立起来。

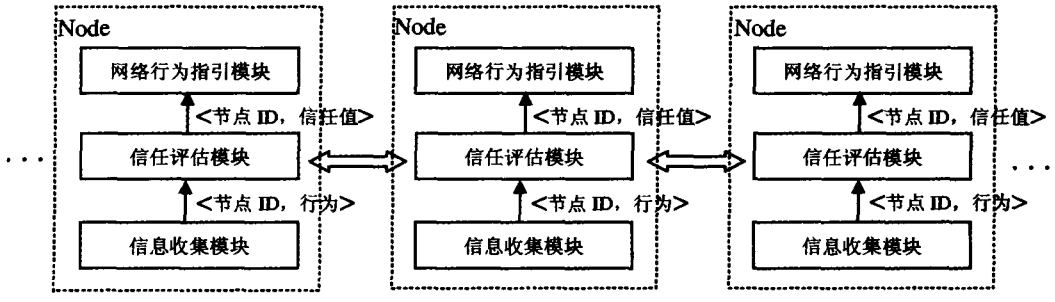

图 1 信任评估系统组成示意图

一个信任评估系统大体包括 3 个模块:信息收集模块、信任评估模块、网络行为指引模块,系统的组成如图 1 所示。其中信息收集模块主要负责收集其他节点的一系列行为,然后由信任评估模块就这些行为进行量化分析,同时和其他节点的信任系统进行交互,最后得到一个信任表,由网络行为指引模块使用,用于指导节点的具体网络行为,比如在进行路由选

*)湖北省自然科学基金(2005ABA243)。洪 亮 博士研究生,主要研究领域为无线网安全;洪 帆 教授,博士生导师,主要研究领域为信息安全;张明猛 助理工程师,主要研究领域为信息安全。余院兰 硕士研究生,主要研究领域为信息安全;

择时，回避那些信任值低的节点等等。

本文通过借鉴人类社会的行为规律，提出移动 Ad hoc 网络中节点之间信任关系的建立、信任度的衡量以及信任评估模型；并通过多角度（直接、间接）评估，来构造一套较健全的信任评估体系，以提高信任评估的准确可靠性。在第 2 节中将详细介绍模型的建立；在第 3 节中详细描述如何综合采用直接信任、间接信任等算法构造完整的信任评估模型；第 4 节通过实例说明对该模型的应用；最后对本文工作进行总结，并展望下一步的工作。

2 信任评估模型

目前，对于信任还没有一个精确的、广泛可接受的定义。但多数学者[6~8]认为，信任是一种主观信念。在 X. 509 的 2000 年版中，对信任的定义为(X. 509,3. 3. 54)“一般来说，如果一个实体假设另一个实体会严格地像它期望地那样行动，那么就称它信任那个实体。”信任包含了双方的一种关系以及对该关系的期望，期望是一个主观的概念。

在本模型中我们引用文[9]的定义，并进行了补充。

定义 1 信任是在不断的交互过程中，某一实体逐渐动态形成的对另外实体的部分或整体的评价，这个评价可以用来指导这个实体的下一步动作。信任具有如下属性：

属性 1 信任度：信任的程度；

属性 2 上下文相关：信任是和上下文相关的，也即和所处的环境相关；

属性 3 多角度：多角度强调信任本身具有多个方面，每个方面都在影响着这个节点是否是可以信赖的；

属性 4 动态性：信任是变化的，不是一旦形成就永久不变的；

属性 5 延迟性：信任是经过不断的学习和经验积累形成的，更新了的信任度只能在下一次的计算中用到。

2.1 实体

信任评估模型的实体对应于移动 Ad hoc 网络中的移动节点，在信任评估中有 3 种角色：评估主体、推荐者、评估客体。网络中的节点能够记录、分类和收集来自推荐者(可信任第三方)所提供的推荐值，并根据推荐者的可信程度决定取舍或进行相关处理，最终给出对客体的信任评估。

2.2 信任类型

信任是上下文相关的，即一个实体对另一个实体的信任是就其能完成某类活动而言的，因而信任应根据不同内容进行分类。在特定环境中，存在多个影响信任关系的因素，这些因素可称为信任属性。信任类型根据信任内容划分，由具体的信任属性刻画。

在移动 Ad hoc 网络中，信任不仅用于处理网络的安全问题，还用于解决其运行的可靠性问题。信任分类将为节点之间的合作和安全决策提供更细致和精确的依据。例如，当需要信任一个节点完成转发数据包的任务时，并不需要信任它能够转发控制包。另外，可以对不同类别的信任分别进行评估，并根据其重要程度的不同进行综合处理。

2.3 信任关系

当实体 i 具有对实体 j 的可信度评价时，则 i 与 j 之间存在信任关系。在本文中，用 $T_{i,j}$ 代表实体 i 对 j 的信任评估。经验是信任评估的主要依据，包括所有的直接或间接的经验。根据经验的来源，信任关系可分为两类：一是直接信任关系，在移动 Ad hoc 网络中，直接信任关系的经验(即样本)可来源于 i 对 j 的信息收集以及网络交互，比如：

①链路帧的接收；

②数据包的中继；

③控制包的中继；

④数据包的接收；

⑤控制包的接收；

⑥信道建立；等等。

二是推荐信任关系，实体 i 具有对 k 提供的关于目标实体 j 的某类经验信息的可信度评估。比如网络中存在 CA，那么 CA 对 j 颁发的证书就具有很高的可信度。

3 信任计算

3.1 直接信任值计算

在这一计算过程中，使用了简单贝叶斯模型方法。根据社会学个人信任行为，在相同环境条件下，实体采取的行为近似于概率 P 的二项事件，因此可利用二项事件后验概率分布服从 Beta 分布的特性推导信任关系。

对于二项分布 $f(y|\theta,m)=\binom{n}{y}\theta(1-\theta)^{n-y}$，当先验概率为 Beta($\alpha$,$\beta$)分布时，其后验概率分布为：

$$P(\theta)=\frac{\Gamma(\alpha+\beta+n)}{\Gamma(\alpha+y)\Gamma(\beta+n-y)}\theta^{\alpha+y-1}(1-\theta)^{\beta+n-y-1}$$

这是参数为($\alpha+y$,$\beta+n-y$)的 Beta 分布，可作为估计后验均值 θ，其中 n 表示总实验次数，y 表示成功次数。若 Beta 先验分布为均匀分布，下一次试验成功概率为：

$$P(event=\mathrm{TRUE}|y,n)=\frac{\Gamma(n+2)}{\Gamma(y+1)\Gamma(n-y+1)}\times\frac{\Gamma(y+2)\Gamma(n-y+1)}{\Gamma(n+3)}=\frac{y+1}{n+2}$$

此概率是对实体未来行为的期望值，可用以表示实体的信任程度。若用 s,f 分别表示成功次数和失败次数，直接信任值可表示为：

$$T^d(s,f)=\frac{s+1}{s+f+2}$$

由于直接信任的经验来自于不同种类，因而计算直接信任值时，本模型对不同种类的经验赋予不同的权值：

$$T^d_{i,j}=\sum_{x=1}^{n}[W_x\times T^d_x(s,f)]$$

其中 x 代表第 x 种直接经验，W_x 代表第 x 种直接经验的权重。

3.2 间接信任值计算

间接信任度的计算采用信任值传递的方法。评估主体 i 对评估客体 j 进行信任评估时，推荐者 k 的推荐值为 $T_{k,j}$，那么 A 所采取的信任值为：

$$T^i_{i,j}=T_{i,k}\times T_{k,j}$$

其中 $T^i_{i,j}$ 代表 i 对 j 的间接信任度，$T_{i,k}$ 代表 i 对 k 的综合信任度；

若 i 没有对 k 的信任评价时，但是有一条路径 l:k_1,k_2,…,k_n 可以获得 k 的推荐信任值，那么此时的间接信任计算公式如下：

$$T^i_{i,j}=T_{i,k_1}\times T_{i_1,k_2}\times\cdots\times T_{k_n,k}\times T_{k,j}$$

简记为 $T^i_{i,j}$，代表 i 从路径 l 对 j 的推荐所获得的间接信任值。

若存在多条推荐路径，可采用权重最大化算法解决，即将每条推荐路径上第一个中间实体信任值作为信任权重，得到多条推荐路径信任合成方法：

$$T^i_{i,j}=\frac{\sum(T_{i,k_1}\times T^i_{i,j})}{\sum T_{i,k_1}}$$

其中 l 代表 n 条不同路径，$l\in\{1,2,3\cdots,n\}$；k_1 则代表路径 l

上的第一个被 i 信任的中间实体。

3.3 综合信任度计算

根据得到的直接信任值和间接信任值，可得到对目标实体总体信任值：

$$T_{i,j}=\alpha T^{d}_{i,j}+(1-\alpha)T^{i}_{i,j}$$

其中 $\alpha\in[0,1]$，代表节点对直接信任值和间接信任值的采信程度，一般由节点自己的策略决定。

4 模型应用举例

为了更好地说明模型，我们将模型应用于 OLSR[10]（Optimized Link State Routing）路由协议中，通过对节点的信任评估，来指导节点的路由选择。

4.1 OLSR 协议简介

OLSR 协议是由 IETF 工作组提出的 4 种应用于移动自组网的基本路由协议之一，该协议隶属于主动式路由协议，节点之间通过定期交换拓扑控制报文来主动获得路由，从而减小通讯链路建立的延迟。OLSR 包含 4 个重要的过程：邻居探测、中继代理选择、路由控制消息的发布、路由表计算等过程。OLSR 通过定期广播邻居探测消息——HELLO 包来发现邻居，HELLO 包含有发布节点 A 的信息以及它的邻居信息。在进行邻居探测过程后，节点将从邻居表根据某种算法选出多点中继代理——MPR。MPR 有两个职责：1）MPR 要负责转发节点的广播报文，节点的其他邻居不能转发，其目的是减小洪泛；2）MPR 要负责在网络中广播它的中继雇主表，其目的是让其他节点知道通过该 MPR 可以到达哪些目的节点。每一个节点选择出 MPR 节点后，会将这一信息反映在下一次的 HELLO 包中。在邻居表更新，进行中继代理选择之后，中继代理节点将定期广播拓扑控制消息，拓扑控制消息中包含发布节点的邻居信息。其它节点收到消息后，根据消息的序列号来决定是否接收该消息。在收到拓扑信息报文后，每一个节点都可以得到一个全局的拓扑网络表，然后利用 Dijkstra 算法计算出到其他节点的最短路径，形成路由表。

4.2 信任产生

4.2.1 直接经验

在 OLSR 中，有以下两方面产生直接经验：

1）确认信息

节点在传输报文成功之后一般会得到一个确认信息。通常这种确认信息有两种渠道获得：一种是链路层的确认帧，这个一般是邻节点在接收到信息之后，会发回一个 MAC 确认包；另一种是网络层以上，当数据传送完毕后，可以要求接收方发回一个确认包。

这种经验主要是来自于数据包的传输，OLSR 的协议控制包都是广播包，因而没有经验。

信任值为：

$$T^{d}_{ACK}(s,f)=\frac{s+1}{s+f+2}$$

其中 s 是传送成功的次数，f 是失败的次数。

2）正确信息

正确的含义不仅包含接收到的数据包的正确性，还包括控制报文的正确性及及时性。比如邻居点 HELLO 包的按时接收等等。为了简单起见，这两种经验作为一种样本空间，不加以区分。

此时信任值为：

$$T^{d}_{ACC}(s,f)=\frac{s+1}{s+f+2}$$

其中 s 是接收信息正确的次数，f 是错误的次数。

4.2.2 间接经验

间接的经验由各个节点产生，一般附加在拓扑控制报文中。通过拓扑控制报文的传播，每个接收节点就获得了发送者对中继雇主（MPR Selector）的评价，从而就获得了间接信任值。

4.3 信任计算

由 4.2 节，根据 3.3 节的计算公式，每个节点都可以计算出其他节点的综合信任度：

$$T_{i,j}=W_{ACK}T^{d}_{ACK}(s,f)+W_{ACC}T^{d}_{ACC}(s,f)+(1-W_{ACK}-W_{ACC})T^{i}_{i,j}$$

W_{ACK} 是确认经验的权值，W_{ACC} 是正确经验的权值。

4.4 路由选择

在进行路由选择的过程中，由于 OLSR 协议是基于链路状态的路由协议，因而每个节点是根据全局拓扑结构来选择路由的。当面临多条路由时，节点应该选择一条可信度高的路径，路径的可信度即是指这条路径所经过的所有节点的综合可信度水平。记路径 l 的可信度为 T_l，其值等于路径所有节点的信任值相乘，公式如下：

$$T_l=\prod_{j\in l}T_{i,j}$$

其中 j 是 l 上的一个节点。

通过公式计算各种路径之后，选择一个值最大的作为路由即可。

总结及下一步工作 由于移动 Ad hoc 网络自身的特点，网络行为需要节点相互协作才能完成，因而节点之间的相互信任对网络的安全保障与可靠运行均具有重要的意义。本文在借鉴人类社会的行为规律的基础上，提出了一个信任评估模型。在这个模型中，节点通过收集评估客体的直接经验和间接经验来构建评价。通过文中的举例，本模型能够很好地与移动 Ad hoc 路由协议相结合，并能对路由机制进行理论上安全的指导。在未来的工作中，关于信任的定义、信任的合理表达等方面还需要深入地研究和探讨。此外，信任模型在实际移动 Ad hoc 网络中应用还需要解决诸如如何合理分类经验信息、如何保障经验信息的可靠传递以及如何搜索经验推荐路径等问题，这些都将是我们进一步研究的内容。

参 考 文 献

1 Buchegger S, Le Boudec J Y. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In: Proc. of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing. Gran Canaria Island: IEEE Press, 2002. 403～410

2 Michiardi P, Molva R. Core: A COllaborative REputation mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In: Proc. of 2002 IFIP Communication and Multimedia Security Conference. Portoroz, Slovenia: Kluwer Academic Publishers, 2002. 107～121

3 Pirzada A A, Datta A, McDonald C. Trust-based routing for ad-hoc wireless networks. In: Proc. of 2004 12th IEEE International Conference on Networks (ICON 2004). Singapore: IEEE Press, 2004. 326～330

4 Pirzada A A, McDonald C. Establishing trust in pure ad-hoc networks. In: Proc. of the 27th conference on Australasian computer science. Dunedin, New Zealand: Australian Computer Society, 2004. 47～54

5 Ren Kui, Li Tieyan, Wan Zhiguo, et al. Highly reliable trust establishment scheme in ad hoc networks. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2004, 45(6): 687～699

6 Beth T, Borcherding M, Klein B. Valuation of trust in open network. In: Proc. of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3～18

7 Jsang A, Knapskog SJ. A metric for trusted systems. In: Global IT Security. Wien: Austrian Computer Society, 1998. 541～549

8 Abdul-Rahman A, Hailes S. A distributed trust model. In: Proceedings of the 1997 New Security Paradigms Workshop. Cumbria: ACM Press, 1998. 48～60

9 王小英，赵海，林涛，等. 基于信任的普适计算服务选择模型. 通讯学报，2005，26(5)：1～8

10 Clausen T, Jacquet P, ed. Optimized Link State Routing Protocol (OLSR). RFC 3626, 2003