第 36 卷 第 7 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.7 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)07—0122—04 文献标识码：A 中图分类号：TP309

基于信任评估的安全路由方案设计

杨成云，张明清，唐 俊
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：分析基于贝叶斯方法的信任评估过程，针对其不能较好反映信任评估的一些重要属性的缺陷，对其信任更新过程进行改进与优化，增强贝叶斯信任评估方法的健壮性和有效性。提出基于贝叶斯方法的信任评估模型和安全路由框架，并实现一种基于 AODV 的安全可信路由方案 TBAODV。仿真实验验证了该方案的有效性。

关键词：Ad hoc 网络；AODV 协议；安全路由；信任；贝叶斯方法

Secure Routing Scheme Design Based on Trust Evaluation

YANG Cheng-yun, ZHANG Ming-qing, TANG Jun
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】This paper analyses the trust evaluation process based on Bayesian approach, aiming at the deficiency that it can't reflect some important attribute of trust evaluation preferably. It improves its trust updating process, boosts up its haleness and validity, and proposes a trust evaluating model and secure routing framework based on the modified Bayesian approach. The paper implements a trust-based routing protocol based on AODV protocol. Simulational experiment proves the validity of the proposed scheme.

【Key words】Ad hoc networks; AODV protocol; secure routing; trust; Bayesian approach

1 概述

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。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，因此移动 Ad hoc 网络相对于有线网更易遭受各种攻击[1]。移动 Ad hoc 网络中所面临的攻击可分为主动攻击和被动攻击，其中，主动攻击又可进一步分为内部攻击和外部攻击，外部攻击是网络外部未授权节点发动的攻击，内部攻击是网络内部被捕获节点或自私节点发动的攻击行为[2]。

当前安全路由方案的设计主要有 2 种方法[3]：一种是基于密码体制的安全路由方案；另一种是基于信任评估的安全路由方案。基于密码体制的方案主要通过加密、认证、数字签名等手段保证路由信息的机密性、完整性和不可否认性等，它虽然能较好地抵制各种外部节点的攻击，但不能有效地防止内部不合作节点的自私行为攻击，并且消耗大量的网络和节点资源。而基于信任评估的方案能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，其作用主要有以下 3 个方面：

(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)从网络中孤立出来。

基于信任评估的安全路由方案一般包括 2 个模块：信任评估模块和安全路由模块。信任评估模块通过监测节点的行为进行量化分析，同时和其他节点的信任系统进行交互，最后得到节点的信任值；安全路由模块主要依据信任评估模块的输出结果如节点信任值进行路由选择，回避那些信任值低的不可靠节点。

2 相关研究现状

针对自私行为等内部攻击的相应方案中，主要有虚拟货币机制(如 Nuglets, Sprite 等)、watchdog-Pathrater 技术、CONFIDANT 机制[4]等。在虚拟货币机制中，需要额外的防篡改硬件(如安全卡)或清算中心(Credit Clearance Service, CCS)，可扩展性差；每个报文都要携带货币，增加了报文的长度及开销。在 watchdog-Pathrater 技术中，Pathrater 只是简单标记了节点的声誉值，没有精确量化信任值，存在一定的检测错误概率。CONFIDANT 机制是在上面方案的基础上增加了 2 个组件，Monitor 用于检测节点行为；Reputation Records 用于记录信任信息；Trust Record 用于控制发送、接收报警信息的情况；Path Manager 使节点根据信任记录情况对路由选择做出调整。其中，信任值的改变只依赖于自己的直接观察所得，不直接发送声誉值，也不借鉴其他节点的信誉值，因此，主观性太强。另外，对于其他节点的报警信息没有进行必要的安全评估，存在错误控告等问题。

在信任评估模型中，由文献[5]分析可知，相对于基于权重的信任模型、基于证据理论的信任模型、基于半环的信任模型和基于主观逻辑的信任模型相比，基于贝叶斯方法的概率模型具有较好的理论基础和较强的实用性，其他方法都存在明显的缺陷或可能产生不合理的结果。但基于贝叶斯方法的信任评估也有自己的不足之处，比如，它不能较好地体现出信任评估的一些重要属性，如时间敏感性等。因此，本文

作者简介：杨成云(1983－)，男，硕士研究生，主研方向：Ad hoc 网络安全，网络仿真；张明清，副教授；唐 俊，讲师
收稿日期：2009-12-10 **E-mail：**yangchengyundemail@163.com

在认真分析信任评估的一些重要属性的基础上，对基于贝叶斯方法的信任评估进行了改进，并提出了一个基于贝叶斯方法的信任评估模型和安全可信路由框架。

3 基于贝叶斯方法的信任评估

3.1 直接信任评估

Bayesian 概率模型[6]是根据现有观察结果集，用概率公式来表达信任。设 x_{AB} 是 B 对 B 的行为(如数据包转发和路由)的评判，0 表示恶意行为，1 表示良好行为。信任是基于历史行为记录集 $D_{AB}=\{x_{AB}(1),x_{AB}(2),\cdots,x_{AB}(n)\mid x_{AB}(i)\in\{0,1\}\}$ 的情况下，一个实体对另一个实体的未来行为的主观期望。设节点的行为正常与不正常服从 β 分布，θ 为节点行为正常的可能性，在 n 次行为中有 α 次正常，β 次不正常行为，$\alpha+\beta=n$，节点间在第 n+1 次行为中正常的概率为

$$p(\theta\mid D_{AB})=Beta(\alpha,\beta)$$

在初始没有任何历史观察行为情况下，θ 服从 0~1 之间的均匀分布，可描述为 $Beta(1,1)$，表示节点可信与不可信的概率相等。观察 n 次行为之后，节点的信任值(trust)可描述为

$$t_{AB}=E(\theta\mid D_{AB})=E[p(x_{AB}(n+1)\mid D_{AB})]=\frac{\alpha}{\alpha+\beta}$$

即信任值取为 β 分布 $Beta(\alpha,\ \beta)$ 的均值。为了增强信任评估的可靠度，基于贝叶斯方法的信任评估过程引入了一个信任值可靠度因子 c(confidence)来描述信任计算的统计可靠性，c 的定义如下:

$$c=1-\sqrt{12}\sigma(\alpha,\beta)=1-\sqrt{\frac{12\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}}$$

其中，c 的值越接近于 1，表明上述所计算的信任值越精确；相反，c 的值越接近于 0，表明计算的信任值可信度越低。但是由 (t,c) 来判断节点的可信度并不直观，为了使基于节点信任度的决策更为方便，由 (t,c) 可以计算出节点最终的可信度值 T，其计算如下:

$$T(t,c)=1-\frac{\sqrt{\frac{(t-1)^2}{x^2}+\frac{(c-1)^2}{y^2}}}{\sqrt{\frac{1}{x^2}+\frac{1}{y^2}}}$$

通过仿真实验得到参数定义为 $x=\sqrt{2},y=\sqrt{9}$ 的仿真实验结果最佳。

3.2 间接信任评估

当节点没有与被评估节点进行交互而缺乏历史行为记录信息或记录信息较少而不能完全真实表达节点之间的信任关系时，须借鉴其他节点关于被评估节点的信任信息来进行评估，这同时也加快了节点信任的收敛速度，使节点之间迅速地建立起可靠的信任关系。间接信任值也被称为推荐信任值。

假设 B 推荐的关于 C 的历史行为记录信息为 $(\alpha_1,\ \beta_1)$，A 当前记录的关于 C 的历史行为信息为 $(\alpha_2,\ \beta_2)$，为了防止不良节点的恶意毁谤攻击(bad mouthing attack)，通过提供不真实的信任信息降低良好节点信任度或增强恶意共谋节点的信任度，必须对推荐信息进行真实性检测。

背离度测试(RC-test):

$$|E(\alpha_1,\beta_1)-E(\alpha_2,\beta_2)|\leqslant\eta$$

其中，$\eta\in(0,\ 1)$ 为背离门限值，如果推荐信任与直接信任接近，则通过检测，接受推荐信息，否则丢弃推荐信息。

间接信任值的计算为

$$T_{AC}=T_{AB}\cdot T_{BC}$$

3.3 总体信任计算

设总体信任值为 T，直接信任值为 T_D，推荐信任值为 T_R，则有:

$$T=\alpha T_D+\beta T_R,\ (\alpha+\beta=1)$$

其中，α 和 β 分别是直接信任和推荐信任的权重，为防止不良节点的恶意诋毁，一般有 $\alpha\geqslant\beta$。

3.4 信任更新过程

假如设 A 对 B 的历史行为记录为 $(\alpha_1,\ \beta_1)$，更新时新产生的正常行为次数和不正常行为次数分别为 r, s，则信任更新方法如下:

新的历史行为记录为

$$\alpha^{new}=\alpha_1+r,\beta^{new}=\beta_1+s$$

相应的新的信任值为

$$t^{new}=E(Beta(\alpha^{new},\beta^{new}))=E(Beta(\alpha_1+r,\beta_1+s))=\frac{\alpha_1+r}{\alpha_1+\beta_1+r+s}$$

然后，根据相应的公式计算可靠度因子和节点新的可信度值。

通过分析可知，当前基于贝叶斯方法的信任更新过程中，对节点行为记录更新时只是进行了直接相加，使得相应的信任值更新过程没有反映出信任评估的以下重要属性:

(1)信任值是时间敏感的，应随时间而变化，而且越近发生的行为对信任值的影响越大。

(2)信任值应该因良好行为增加得慢，因恶意行为减少得快(信任建立难，失去容易)，这样会加快恶意节点的检测速度，及早地发现恶意行为，同时也迫使节点持续递进行协作才能获得良好的信任值。

(3)信任评估应激励节点具有良好的整体信任历史。对于同一良好行为，整体信任历史记录越好的节点，信任值增加得越快；对于同一不正常行为，整体信任历史记录越好的节点，信任值减少得越慢。

(4)信任评估应该可以根据具体应用环境进行重新调整，以满足不同应用的需求。

为了使基于贝叶斯方法的信任评估过程满足以上特性，对基于贝叶斯信任评估的更新过程进行改进，引入一个优化处理过程，其改进如下:

(1)为了体现信任值的时间敏感特性，减少过去行为信息对当前信任值的影响，增加最近发生事件的权重，引入一个指数衰减因子(遗忘因子)来减少过去行为的影响。

(2)为了体现信任建立难失去容易的特性，引入了奖赏因子和惩罚因子，且惩罚因子大于奖赏因子。

(3)通过一个整体历史良好率来激励节点具有良好的信任历史。

改进后的信任更新过程如下:

$$\alpha^{new}=\alpha_1 e^{-c\Delta t}+RWD(1+RAT)\cdot r$$

$$\beta^{New}=\beta_1 e^{-c\Delta t}+PNT(2-RAT)\cdot s$$

$$t^{new}=E(Beta(\alpha^{new},\beta^{new}))$$

其中，c 为指数衰减系数；RWD 为奖赏因子；PNT 为惩罚因子；RAT 为节点整体历史行为良好率，$RAT=\frac{\text{所有良好行为数}}{\text{所有行为记录数}}$。

在上述更新公式中，引入了指数衰减方法来遗忘过时的历史行为记录，这样会给最近行为事件更多的权重，更好地体现节点当前的行为特点；由于引入了奖赏因子和惩罚因子，

并且惩罚因子大于奖赏因子，对于同一个节点，因一个恶意行为减少的信任值要比一个良好行为增加的信任值大，因此一个恶意行为给节点的带来的负面影响比一个良好行为给节点带来的正面影响大，当节点出现恶意行为时，信任值会迅速减少，恶意攻击节点会迅速地被发现，因此，会激励节点持续的进行协作。*RAT* 为节点过去行为的整体良好率，过去行为整体表现越好的节点因良好行为所增加的信任值越大，因不正常行为而减少的信任值越小，这样也会鼓励节点协作来拥有良好的历史行为记录。因此，改进后的信任评估过程能更好地反映节点的行为特点，使基于贝叶斯方法的信任评估更为健壮有效。

这些参数也可以按照具体应用的需要进行调整，如当一个节点由于环境的影响使得它的行为不断地改变，这里可以考虑调整遗忘因子，使得最近的行为获得更多的权重；又如如果节点经常地加入和离开系统，可以考虑增加奖惩因子，使新进入的节点能够迅速地建立起足够的信任值，这也充分表明了此信任模型的灵活性。

4 基于信任评估的安全路由协议

4.1 信任评估模型及安全路由框架

上面对基于贝叶斯方法的信任评估过程进行了优化与改进，在此基础上提出一个基于贝叶斯方法的信任评估模型及安全路由框架，如图 1 所示。

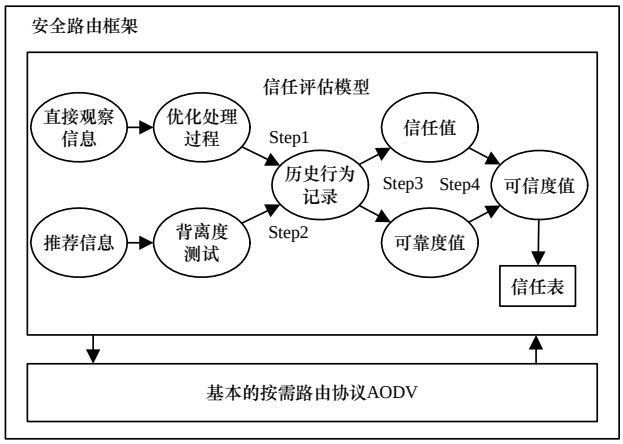

图 1 信任评估模型和安全路由框架

信任评估模型的简单描述如下:

Step1 通过直接观察信息更新历史行为记录信息，节点通过看门狗(watchdog)等机制监测邻居节点的行为。在此过程中，引进了一个优化处理模块，根据行为发生的时间和节点过去行为特征等信息优化了信任更新过程。

Step2 散布和处理推荐信息，每个节点周期性地公布自己关于其他节点的信任信息，同时也收到邻节点公布的推荐信息，一个节点观察到的关于自己邻节点的直接信息可以被其他节点所利用，这种信任共享机制使得对一个节点的信任评估更加全面，同时也加速了信任的收敛过程，使节点间的信任关系能够迅速建立。当收到邻居节点的推荐信息时，要对推荐信息进行真实性检测。

Step3 信任值和可靠度值计算。信任值描述了某一节点基于历史行为记录对另一节点正常完成某个功能的信任程度。可靠度值描述了所计算的信任值的精确性与可靠性，一个较高的可靠度值表明被评估节点通过了评估节点和其他节点的大量检验，因此，相应的信任值更加可靠。其中，信任值是通过计算 Beta 分布的期望值所得，可靠度值的计算与 Beta 分布的标准差相关。

Step4 由信任值和可靠度值计算出可信度值。通过对 Step3 中所计算的信任值和可靠度值结合成一个对节点的最终总的评价值——可信度值。

基本的路由协议以信任评估模块的输出为依据，通过查看邻居信任表进行路由选择，同时信任评估模块通过监测节点执行路由协议的情况进行相应信任评估。

4.2 TBAODV安全路由协议

本文在按需路由协议 AODV 的基础上进行改进，增加信任评估机制，提出基于信任评估的安全可信路由协议 TBAODV(Trust-Based AODV protocol)。

当源节点 *S* 要寻找到达目的节点的路径时，发起一个路由发现过程。所设计的路由发现算法的基本思想如下:

(1)一条路径的可信度由本路径中可信度最低的节点信任度决定，即:

$$route\_trust=\min\{node\_trust(i),\ i=1,2,\cdots,n\}$$

(2)当有多条到达目的节点的路径时，选择可信度最高的路径进行数据传输。

(3)当有多条路径的可信度相同时，再依据跳数值选择最短路径进行数据传输。

因此，在路由发现过程中，对路由请求数据包 RREQ 进行了扩展，增加了路径可信度数据项。当中间节点收到路由请求包时，把发送给它 RREQ 数据包的上一跳邻居节点的信任值与 RREQ 请求包中的路径可信度 *route_trust* 进行对比，如果上一跳邻居节点的信任值比 *route_trust* 小，则用上一跳邻居节点的信任代替 *route_trust* 值，否则不改变 *route_trust* 值。

当中间节点收到路由请求数据包时，其处理过程简单描述如下:

(1)查看自己是否为目的节点，如果是目的节点，则选择信任度最高的路径进行回复，如果存在多条信任度相同的路径，则依据跳数计数器选择最短路径进行回复，如果不是目的节点，则进行下一步处理。

(2)检测是否是重复包，如果是重复包，则丢弃，如果不是，则进行下一步处理。

(3)查看邻居节点信任表，比较上一跳节点的可信度和路由请求数据包中路径信任度，如果上一跳邻居节点的信任度比请求包中的路径信任度小，则更新路径信任度，否则不改变 *route_trust*。

(4)增加跳数值，建立反向路径，继续广播路由请求包。

路由回复的处理过程与路由请求处理过程相似，这里不再进行详细描述。当源节点收到路由回复后，查看路由回复包(RREP)中的路径可信度，如果路径可信度满足自己安全需求的最低门限值，则进行数据传输，否则，重新发起路由请求过程。

在路由维持阶段，在 AODV 路由协议中，当发现路径中的链路发生中断时，会通过发送路由错误信息 RRER 通知上游节点删除相应的路由表项。在 TBAODV 中，当某节点发现路由路径中的邻居节点的信任值低于阈门值即被发现为不合作节点时，也会发送 RRER，以删除无效的路由。

5 仿真实验

为了验证所提信任模型和安全路由协议的有效性，本文

使用源代码公开、具有良好扩展性的仿真软件 NS2 进行仿真实验，在不同数量的不合作恶意节点环境中，分别模拟了 TBAODV 安全可信路由协议和原 AODV 路由协议下网络的运行状况。基本实验参数如表 1 所示。

表 1　仿真实验参数

参数	对应值
总节点数	50
不合作节点娄	0~16 可调
仿真空间	1 500×1 500
仿真时间/s	800
流量类型	CBR
分组传输速率/(packer·s^{-1})	4
分组大小/Byte	512
移动模型	Random way point
最大移动速率/(m·s^{-1})	0~20
带宽/(Mb·s^{-1})	2
节点通信范围/m	200

主要参数和阈值的选取：

(1)在总体信任值的计算公式中，为了防止不良节点的恶意信任诋毁，取 $\alpha = 0.7, \beta = 0.3$，即直接信任的权重比推荐信任的权重大。

(2)可信与不可信阈值的确定。对信任值 t 和可靠度因子 c，在初始没有任何历史行为经验时，有 t=0.5, c=0，即节点成功转发包的机率为 50%，这时可以得到节点可信度值 T 为 0.378 4。经过分析，从一开始节点就不断丢包，当丢包数达到 5 时，节点可信度降到 0.3 以下。因此，选取 0.3 作为节点可信与不可信的阈值。

(3)指数衰减系数 c=1，奖赏因子 RWD=1，惩罚因子 PNT=2.5。

仿真实验选择以下性能指标进行比较：

(1)分组投递率：成功到达目的节点的分组数与源节点所发送的分组数之比。

(2)丢包率：恶意节点丢弃的分组数与所有发送的分组数之比。

(3)路由开销：为完成路由功能而额外传送的控制分组数与传输分组总数之比。

以下是仿真结果及分析：

(1)分组投递率。由图 2 可知，随着不合作节点的增多，丢包行为也不断增多，使得 2 种协议的分组投递率都有不同程度的下降，当不合作节点达到 1/3 时，原 AODV 路由协议的分组投递率只有 30%，严重影响网络的正常工作；但 TBAODV 路由协议的分组投递率明显优于 AODV，在不合作节点达到 1/3 的情况下，还能保持较高的分组投递率，这主要是由于 TBAODV 路由协议选择可信度高的节点进行路由的建立，避免了不合作节点出现在路由路径上，使建立的路由更加稳定可靠。

(2)丢包率。由图 3 可知，随着不合作节点的增加，丢包率不断增大，特别是原 AODV 路由协议在恶意节点数达到 10 时丢包率急剧增加，最高达到 65%。而 TBAODV 协议会根据节点的信任值将不合作节点排除在路由路径之外，对恶意节点的使用率明显减少，因此，它的丢包率比 AODV 路由协议小得多。

(3)路由开销。由图 4 可知，安全可信路由协议 TBAODV 的路由开销比原 AODV 路由协议稍高一点，这是由于在 TBAODV 的协议中，根据节点的信任值可以在较短时间内判断出哪些是不良节点，从而避免这些节点参与路由，但因此会使网络中的可用节点减少，从而增加 RREQ 的发送；另一方面，在路由维护阶段，当发现不合作节点时，节点也会发送 RRER 信息来通知其他节点删除相应路由，因此，也增加了路由控制信息的开销。

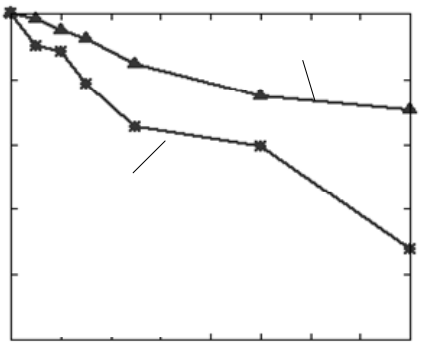

图 2　分组投递率

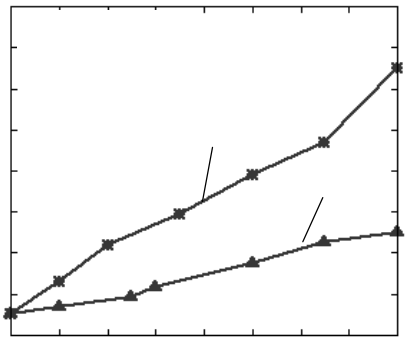

图 3　丢包率

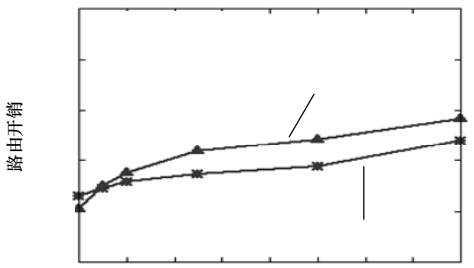

图 4　路由开销

由上面的仿真实验可知，TBAODV 安全路由方案以很少的代价，为移动 Ad hoc 网络建立了一条安全可信的路由。

6　结束语

移动 Ad hoc 网络的建立与运行需要节点相互协作才能完成，因此，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。本文分析基于贝叶斯方法的信任评估过程，并对其更新过程进行改进与优化，使它能够更好地满足信任的一些重要属性，增强信任评估的健壮性和有效性。

（下转第 128 页）