基于信任距离的车联网恶意节点检测方法

邬海琴 王良民
(江苏大学计算机科学与通信工程学院 镇江 212013)

摘 要 针对车联网网络拓扑结构变化快且相比传统移动自组网络更易受到恶意车辆发起的内部攻击等问题,在当前贝叶斯假设的信任理论研究的基础上,结合车联网高速移动中快速检测恶意节点的要求,加大否定事件的影响力度,提出了用于评估车辆节点行为的信任模型;在综合推荐信任值时,引入了"推荐信任距离"作为推荐信任的信任度量,预先排除恶意推荐意见,并有效防止车辆的串通攻击。与现有的基于信任的检测方法相比,该方法加快了检测速度,并简化了推荐传递。仿真实验表明,该方法有较快的检测速度,从网络丢包率和恶意节点检测率可以看出此信任模型对检测恶意节点具有较好的性能。

关键词 车联网,信任模型,贝叶斯假设,推荐信任距离,网络丢包率,检测率
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.033

Trust Distance Based Malicious Nodes Detection Method in Vehicular Ad Hoc Network

WU Hai-qin WANG Liang-min
(School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract With the requirement of rapid detection of malicious nodes in high-speed VANET, a trust model was proposed on the basis of bayes hypothesis, aiming at solving the issues that the topology of VANET changes quickly and is more vulnerable to malicious internal attack than traditional mobile ad-hoc network. The model intensifies the influence of negative events, to eliminate the malicious recommendations in advance and avoid collusion attack. The concept of "recommendation trust distance" is introduced as trust metric of recommendation trust when integrating recommendation trust. Compared with the current detection method based on trust, this model speeds up the detection speed and simplifies the recommend delivery. The simulation experiment shows that this trust model has rapid detection speed and good performance in detecting malicious nodes from the network packet loss rate and the detection rate of malicious nodes.

Keywords VANET, Trust model, Bayes hypothesis, Recommendation trust distance, Network packet loss rate, Detection rate

1 引言

车联网作为无线自组织多跳网络在智能交通领域的延伸和应用拓展,具有非常广阔的应用前景[1]。V2V(Vehicle to Vehicle)和V2I(Vehicle to Infrastructure)是车联网的两种主要通讯模式,采用IEEE 802.11p作为底层协议的专用短距离通信技术DSRC(Delicated Short Range Communnication),能够提供车辆在高速运动下的数据传输。

车联网除了具有一般移动自组织网络的自组性、多跳性、无中心等特点,由于车辆高速移动与道路分布、地理环境密切相关,还具有网络拓扑结构变化快、无线信道质量不稳定等特征,因此更易受到网络外部和内部的安全威胁,如恶意车辆节点散布虚假信息扰乱交通;为节省自身的能源,部分自私的车辆节点拒绝转发其他车辆发送的信息,导致关键信息无法传递,网络传输性能大大下降。传统的安全机制主要依赖可信的第三方即数字证书认证中心CA(Certificate Authority)来进行加密和验证,实现网络安全接入[2],从而保证通信的可靠性,但由于车联网的无中心、网络开放、非可靠传输等特点,传统安全机制无法解决网络内部节点的恶意行为;而在移动自组网中,主要将信任和信誉作为保障自治网络安全的一个重要手段,许多研究者也提出了相关的信任管理模型用于检测恶意节点[3-5],将信任主要分为直接信任和推荐信任,但推荐信任中大多采用节点传递推荐,计算较复杂,且增加了时延,难以满足车辆在高速移动中快速检测恶意节点的要求。因此,设计合理的信任模型对解决车联网安全问题和促进车联网在智能交通领域的发展具有重要意义。

本文针对当前信任理论存在的缺陷,并结合车联网高速移动中快速检测恶意节点的要求,一方面,对当前信任管理模

到稿日期:2014-08-29 返修日期:2014-11-07 本文受国家自然科学基金(61272074),江苏省自然科学基金(BK2011464),镇江市工业支撑计划项目(GY2013030)资助。
邬海琴(1992-),女,硕士生,主要研究方向为车联网通信安全,E-mail:whq02197169@sina.com;王良民(1977-),男,博士后,教授,CCF高级会员,主要研究方向为无线传感器网络及安全协议。

型进行改进，引入否定事件影响因子 λ 来增加恶意行为的权重，使信任值快速收敛到阈值以下，从而更快地发现恶意节点；另一方面，提出“推荐信任距离”的概念作为推荐信任的信任度量，即推荐信任的可信度，提前排除不合理的推荐意见，在加快信任计算及检测速度的同时，有效抵制了车辆节点的串通攻击。

本文第 2 节介绍了当前无线传感网、移动自组网以及车联网中的信任管理模型；第 3 节介绍了信任关系分类并提出了适用于车联网的信任评估模型；第 4 节进行仿真实验并分析模型对检测恶意节点的性能；最后对全文进行总结。

2 相关工作

信任管理系统在网络安全中扮演了重要的角色，因此有关信任管理的研究也得到了许多关注。当前相关的工作主要是在各种网络环境中建立适当的信任评估模型或设计基于信任的路由协议[6-8]用于检测恶意节点。目前在无线传感网和移动自组网背景中提出的检测恶意节点的信任模型已比较成熟，但在新兴的车联网背景中提出的信任模型还尚在研究阶段。

早期，A. Josang 提出了基于主观逻辑的信任模型[9]，以 beta 分布函数描述二项事件后验概率的思想，得到由观察到的肯定事件数和否定事件数来确定的概率确定性密度函数，并以此计算实体产生某个事件的概率可信度，总结出信任具有主观性和不确定性。

文献[10]提出了无线传感网络中分层的信誉模型，首先将所有节点分簇，采用 leach 算法选出簇头，从而将传感器网络分为基站、簇头节点层和普通节点层，由簇头节点对普通节点进行管理，在此基础上对节点行为属性和网络攻击进行建模。虽然此模型应用于无线传感网中具有很好的检测效果，但在车联网高速移动的环境中，leach 算法并不完全适用，因此存在分簇算法选取以及簇头选择的问题。移动自组网中的信任评估方法很多，按其研究方法的不同主要分为两类：通过环或链迭代计算信任的流模型[11]和基于统计学的概率论模型[12]。前者主要采用半环代数理论来抽象信任计算过程，根据中间节点的信任度计算源节点对目的节点的信任度，但没有考虑信任随时间变化的特性；后者虽使用马尔可夫链分析了节点信任值随时间的变化，但其对信任评价只用 1 和 −1 来区别，过于简单，因此系统通用性很差。

在车联网中，文献[13]提出了基于事件的信誉模型来排除恶意节点发送的虚假信息，此模型将遇到同一交通事件的车辆分为 3 种角色：事件报告者、事件观察者和事件其他参与者。3 种角色对事件的信任计算互不相同，其中观察者是识别虚假信息的主要角色，其接收来自报告者和其他观察者的事件信任值，并结合报告者随后的行为计算自身对事件的信任值来评估事件信息。但此模型只能由观察者检测出虚假事件信息，报告者一跳范围外的其他参与者无法直接识别虚假信息，且其对其他行为的恶意节点也无法检测。

文献[14]提出的层次分析的信任管理模型主要将信任评估分为 3 步：信誉计算、直接信任计算以及间接信任计算。其虽然根据车辆身份的不同考虑了车辆节点本身的信誉值，使得信任评估更加全面，但在信任组合时只是简单将这 3 种信息相加，并没有考虑权重问题，忽略了车辆恶意推荐及串通攻击的可能；另一方面其也未考虑信任动态变化的特征，缺少信任值的更新过程。

田俊峰等[15]提出的基于推荐的信任链管理模型通过构建信任网络，利用加权紧密度对信任链上的推荐信任进行合并，但由于存在推荐传递，因此大大增加了模型的计算量。

本文针对目前信任管理模型的研究现状及存在的问题，结合车联网特殊环境以及快速检测恶意节点的要求，对当前信任管理模型进行改进，并针对车联网中的恶意自私节点提出基于信任距离的检测方法。

3 基于经验贝叶斯假设的信任模型

3.1 信任理论

在人类社会中，信任是最常见的概念之一，具有主观性、模糊性和不确定性。早前，Mui 等[16]对信任是这样定义的：信任依赖于经验并随时间变化，当两个人相遇时，他们对彼此的态度受以前经验认识的影响，这是主体对客体的直接认识，在信任评估中还有一种角色：推荐者，其主要作用是降低主体对客体给出的直接信任评估的不确定度。社会关系中的信任评估可以按照以下方式进行：首先主体可以根据对客体的历史表现经验直接给出信任评价，主体若不认识客体，或为了降低主体直接信任评估的不确定度，则可以参考自己认识的并且也认识客体的人给出的推荐意见，最后将直接信任和推荐信任按一定权重综合得到总体信任值。参照上述信任评估方式，可以将网络中节点间的信任关系分为直接信任和推荐信任。

3.2 信任评估模型

在车联网中，节点的历史行为具有统计意义，网络中的某些恶意车辆节点如自私车辆为了节省自身能源，而选择不转发收到的信息，在其历史行为总表现为恶意丢包的情况下，它的下一个行为是恶意的概率较高。概括来说，信任是基于历史行为的情况下，一个实体对另一个实体未来行为的主观期望。由于经验贝叶斯估计的评估过程非常接近于人们日常生活中获得概率信息的情况，因此本文采用经验贝叶斯估计对节点的行为进行概率上的判断，量化节点行为来计算节点直接信任值，并针对车联网高速移动中快速检测恶意节点的要求，引入否定事件影响因子 λ 来增加恶意行为的权重，使信任值快速收敛到阈值以下。

3.2.1 直接信任值

通过观察和交互，主体 S 观察得出客体 X 为正常节点的概率是 θ，根据 Bayes 定理在初始没有历史交互行为的情况下，$\theta \sim U(0,1)$，即先验概率服从均匀分布。记历史交互成功次数为 u，失败次数为 f，本文中交互成功是指客体 X 成功转发了其所接收的信息，反之则认为交互失败。在一段时间内经过 x 次交互后，统计得出 $\theta \sim \text{beta}(u+1, f+1)$，即后验概率服从 beta 分布，其密度函数为：

$$P(\theta)=\frac{\Gamma(u+f+2)}{\Gamma(u+1)\Gamma(f+1)}\theta^{u}(1-\theta)^{f} \tag{1}$$

由式(1)对未来事件进行预测，则下一次交互成功的概率可以看成 beta 分布的期望：

$$P=E(\beta(u+1,f+1))=\frac{u+1}{u+f+2}=\frac{u+1}{x+2} \tag{2}$$

式(2)是对 X 未来行为的期望。参照信任的定义，可以将其用来表示 S 对 X 的直接信任评估，即

$$T_d=\frac{u+1}{u+f+2} \tag{3}$$

由于车联网中车辆移动速度非常快，因此通信链路的寿命相对较短，这就要求车联网比移动自组网有更快的检测速度。

现实生活中，我们对一个人的信任是在认识的过程中慢慢建立起来的，不会因为对方做了一件肯定的事就大大增加对他的信任度；相反，我们会因为对方做了一件否定的事而迅速降低对他的信任。由此可以看出，在同等条件下，信任值因良好行为增长得慢，因恶意行为下降得快；MIT 的 C. Dellarocas[17] 也认为从主观角度来说，否定事件对信任的影响力度要大于肯定事件。而式(3)表示肯定事件和否定事件具有相同的权重，为了加大否定事件的的影响力度，快速地使信任值收敛到信任阈值内，从而加快检测出恶意节点，本文引入否定事件影响因子 λ 来对原先的贝叶斯模型进行改进，加大否定事件的影响力度。修正后的信任评估值为：

$$T_d=\frac{u+1}{u+\lambda f+2},\lambda \text{ 为常数且} \lambda>1 \tag{4}$$

网络中的每个车辆节点都有一张信任信息表，用来记录与其有过交互的车辆的直接信任值，计算方法由式(4)得到。

3.2.2 推荐信任值

为了减少推荐传递带来的复杂计算，本文只考虑主体一跳范围内邻节点的推荐意见，如图 1 所示。

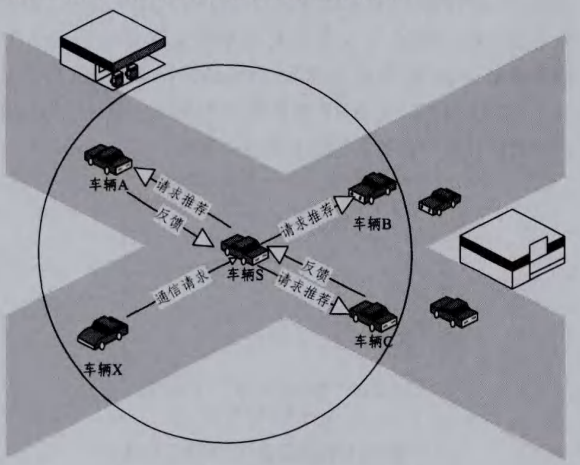

图 1 信任推荐示意图

车辆 X 向 S 发出通信请求，S 先计算对 X 的直接信任值，再向其邻居节点 A、B、C 发出推荐请求，邻居车辆 A、C 若与 X 有过历史交互行为，则把对 X 的直接信任评估作为推荐反馈给 S。

在反馈推荐信任的过程中，某些恶意车辆可能会故意给出较低的信任值，当推荐车辆节点个数较多时，一个低信任推荐可能对车辆 X 的总体评估影响不大，但当多个恶意车辆合谋给出低推荐信任时，S 对 X 的信任评估就会受到影响。为防止 S 接收不合理的推荐意见，本文引入“推荐信任距离”的概念作为推荐信任的信任度量，即推荐信任的可信程度，预先排除可信度很低的推荐信任值，以有效抵制恶意车辆节点的串通攻击。节点 i 和节点 j 对节点 X 的推荐信任距离可由下式计算得到：

$$D_X(i,j)=|T_{d(i,X)}-T_{d(j,X)}| \tag{5}$$

其中，$T_{d(i,X)}$、$T_{d(j,X)}$ 分别为 i、j 对 X 的直接信任值，即反馈给 S 的推荐信任。

假设节点 S 一跳范围共有 N 个邻节点 $k_1,k_2,\cdots,k_i,\cdots,k_N$，其中节点 k_i 为节点 S 最信任的邻节点，T_{refer} 为推荐信任参考值，$T_{r(k_j)}$ 表示节点 k_j 对 X 的推荐信任值，推荐信任距离的阈值为 d。恶意推荐意见排除的具体伪代码如算法 1 所示。

算法 1 恶意推荐意见排除伪代码

```
1. Begin
2. find node k_i among the neighbors of node S
3. T_refer ← T_d(k_i,X)
4. D_X(k_j,k_i) ← |T_d(k_j,X) − T_refer| (j=1,2,…,N & j≠i)
5. If D_X(k_j,k_i) < d Then
6.    T_r(k_j) ← T_d(k_j,X) (keep)
7. Else
8.    T_r(k_j) ← 0(delete)
9. End If
10. End
```

将 S 最信任的邻节点 k_i 给出的推荐信任作为参考，若其他节点 k_j 与其推荐信任距离小于阈值 d，则说明 k_j 的推荐信任是可信的，否则不可信并排除。

算法 2 中，第 2 行代码找出 S 最信任的邻节点 k_i，m 为节点 S 直接信任表的总长度。

算法 2 search k_i

```
1. Begin
2. Input Trust table of node S
3. T_d(S,k_i) ← T_d(S,k_1)
4. For j=2 to m
5. If T_d(S,k_j) > T_d(S,k_i) Then
6.    T_d(S,k_i) ← T_d(S,k_j)
7. End If
8. End For
9. Return k_i
10. End
```

按下式将邻居节点合理的推荐意见进行综合：

$$T_r=\frac{\sum_{i=1}^{N}(T_{d(S,k_j)}\times T_{r(k_j)})}{\sum_{j=1}^{N}T_{d(S,k_j)}} \tag{6}$$

其中，$T_{d(S,k_j)}$ 为节点 k_j 推荐值的权重，即节点 S 对它的直接信任评估值，$T_{r(k_j)}$ 为节点 k_j 的推荐信任值。

3.2.3 信任信息组合

用信心值 f 作为权重来组合信任信息，f 为主体 S 给出的对客体 X 的直接信任评估的确定度，f 越大，则 S 对 X 的直接信任评估越确定，推荐信任的作用就越小。信任信息组合的公式如下：

$$T=f\times T_d+(1-f)\times T_r \tag{7}$$

其中，T_d 为直接信任值，T_r 为推荐信任值。信心值 f 采用模糊信任模型[18]中信心值的计算方法，记 S 与 X 进行交互的事件全集 $E=\{e_1,e_2,\cdots,e_n\}$，集合 $V=\{v_1,v_2,\cdots,v_n\}$，$P(E)$ 为 E 的幂集，$X\in P(E)$ 是主体 S 持有的证据事件。信心值 $f(X)$ 由以下公式给出：

$$f(X)=\begin{cases}\dfrac{|X|}{|E|}, & \forall e_i\in X, v_i=1\\ \dfrac{|X|}{2|E|}, & \exists e_i\in X, v_i=-1\end{cases} \tag{8}$$

其中，$v_i=1$ 表示事件 e_i 成功，$v_i=-1$ 表示事件 e_i 失败。

3.2.4 信任更新

由于信任是动态变化的且近期经验要比历史经验更为可信，因此引入时间遗忘因子 μ 作为权重参数。更新后的信任值 T 为：

$$T=\mu\times T_{new}+(1-\mu)\times T_{old} \tag{9}$$

其中，T_{new} 为近期信任值，T_{old} 为历史信任值，且 $\mu>0.5$。

4 仿真实验与分析

利用 VanetMobiSim 交通仿真器和 NS2 进行联合仿真，VanetMobiSim 生成 NS2 所需的车辆运动场景文件。在 AODV 协议中添加恶意丢包节点，修改路由代码后重新编译，设置车联网通信场景参数和业务流数据，模拟车辆间的通信。仿真实验通过编写 awk 程序来分析 trace 文件获取节点通信成功、失败的次数，将其作为信任评估模型的数据来源。

实验共设置 50 个车辆节点，其中恶意节点为 5 个，将仿真时间依次设置为 50s、100s、150s、200s、250s、300s，信任评估模型的参数设置见表 1。仿真各个时间段的通信情况，算出节点信任值，图 2 所示为选出的两个正常节点和恶意节点的信任值变化情况。

表 1 参数设置

主要参数	参考值
否定事件影响力度 λ	2
推荐信任距离阈值 d	0.2
时间遗忘因子 μ	0.6
信任阈值	0.4
信任更新周期	50s

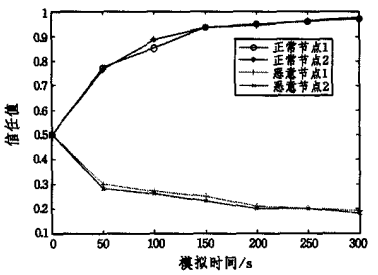

图 2 正常节点与恶意节点信任值的比较

图 2 显示，随着时间的推移，正常节点信任值呈上升趋势，300s 时信任值已达到 0.98 左右，远高于信任阈值；而恶意节点在 300s 时信任值下降到 0.2 左右，低于了信任阈值。由此可以看出，此信任模型能够将信任值低于阈值的恶意节点检测出来。

图 3 是传统贝叶斯模型和引入否定影响因子的改进模型对节点信任值影响的比较。可以看出，改进模型经过第一个周期 50s 后信任值就降到 0.3 以下，低于信任阈值，即一个周期就能检测出恶意节点，而传统的贝叶斯模型要 3 个周期 150s 后才能检测出恶意节点。因此，改进后的模型能更快地检测出恶意节点。

图 4 主要比较两组实验下网络丢包率的情况。丢包率指的是接收节点丢失包的总数与发送节点发送包的总数的比值。一组是在选取路径时，不考虑节点的信任值；另一组是在每周期信任更新后，低于信任阈值的节点不再加入到网络中。由图可以看出，排除恶意节点后，网络丢包率明显低于未排除恶意节点的情况，这与实验中的恶意节点设置为恶意丢包相一致。

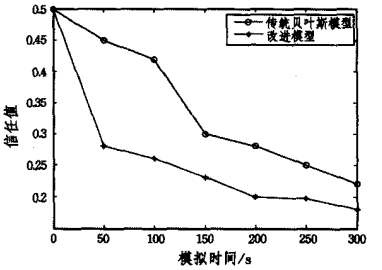

图 3 贝叶斯模型与改进模型对恶意节点信任值影响的比较

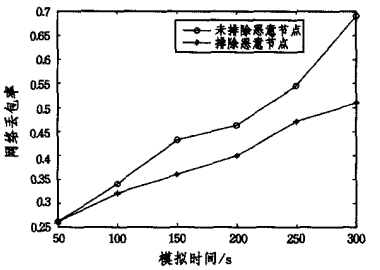

图 4 网络丢包率比较

图 5 给出了现有的基于 AHP[14] 的信任模型和本文模型在不同恶意节点数目下的检测率比较。恶意节点检测率定义为一段时间内检测出的恶意节点数与预先设置的总的恶意节点数的比值。可以看出，在恶意节点数目增多时，两种模型的检测率均有所降低，但本文方案明显优于 AHP 信任模型，随着恶意节点的增加，本文模型检测率的下降速度小于 AHP 信任模型，在恶意节点数达到 20% 的情况下，检测率仍在 96.5%以上，较高，而 AHP 信任模型检测率已低于 94%，说明本文信任模型检测恶意节点的性能较好。

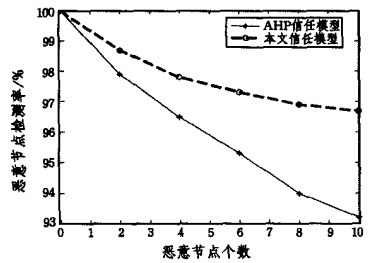

图 5 不同信任模型恶意节点检测率的比较

结束语 本文在当前信任理论研究的基础上，结合车联网网络拓扑结构变化快、要求快速检测恶意节点的特性，引入否定事件影响因子，使节点信任值快速收敛；推荐信任评估中，主要考虑主体一跳范围内邻节点对客体节点的信任推荐，简化了复杂的推荐传递，同时在信任的基础上引入“推荐信任距离”作为推荐信任的信任度量，预先排除可信度很低的推荐信任值，有效抵制了恶意车辆节点的串通攻击。

在仿真实验中，从网络丢包率和恶意节点检测率两方面来评估信任模型的性能。实验结果显示，此信任模型能够较快地检测出恶意节点，并且恶意节点检测率也很高。

与现有的信任模型相比，本文提出的信任模型适用于车联网通信环境，且计算简单，相比传统模型，加快了恶意节点的检测速度；本文方案也有值得改进的地方：目前恶意节点的行为只是设置为恶意丢包，对其他攻击如数据篡改等还需要进一步验证。

（下转第 174 页）

Evolutionary Computation. 2007:49-56

[10] Greensmith J, Aickelin U, Twycross. Articulation and Clarification of the Dendritic Cell Algorithm [C]// Artifical Immune Systems: Proceedings of the 5th International Conference on Artificial Immune Systems(ICARIS). Springer, 2006:404-417

[11] Oates R, Greensmith J, Aickelin U, et al. The Application of a Dendritic Cell Algorithm to a Robotic Classifier [C]// Artificial Immune Systems: Proceedings of 6th International Conference on ICARIS 2007. Springer, 2007:204-215

[12] Al-Hammadi Y, Aickelin U, Greensmith J. DCA for bot detection [C]// Evolutionary Computation(CEC 2008). 2008:1807-1816

[13] Vella M, Roper M. Characterization of a danger context for detecting novel attacks targeting Web-based systems [EB/OL]. http://www.cis.strath.ac.uk/~mv/trep2.pdf. 2010

[14] 陈慰峰. 医学免疫学[M]. 北京:人民卫生出版社, 2000
Chen Wei-feng. Medical Immunology [M]. Beijing: People's Medical Publishing House Press, 2000

[15] Li Y, Chen J, Gong P, et al. Study on Land Cover Change Detection Method Based on NDVI Time Series Datasets Change Detection Indexes Design [J]. Journal of Basic Science and Engineering, 2005, 13(3):261-275

[16] Yang Chao, Liang Yi-wen, Liu Ao-lin. The Danger Sensed Method by Feature Changes [J]. Energy Procedia 13, 2011:4429-4437

(上接第 160 页)

参 考 文 献

[1] Fazio P, De Rango F, Lupia A. A new application for enhancing VANET services in emergency situations using the WAVE/802.11p standard[C]// Wireless Days(WD), 2013 IFIP. IEEE, 2013:1-3

[2] 乔震,刘光杰,李季,等. 移动自组织网络安全接入技术研究综述[J]. 计算机科学, 2013, 40(12):1-8, 30
Qiao Zhen, Liu Guang-jie, Li Ji, et al. Survey on Secure Access Technology in Mobile Ad-hoc Network[J]. Computer Science, 2013, 40(12):1-8, 30

[3] Sharma S, Mishra R, Kaur I. New trust based security approach for ad-hoc networks [C]// 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT). Chengdu, 2010, 9:428-431

[4] Xia H, Jia Z, Sha E H M. Research of trust model based on fuzzy theory in mobile ad hoc networks[J]. IET Information Security, 2013, 8(2):88-103

[5] 陈深龙,张玉清. 增强 ad hoc 网络可生存性的健壮多维信任模型[J]. 通信学报, 2010(5):1-9
Chen Shen-long, Zhang Yu-qing. Robust multi-dimensional trust model for improving the survivability of ad hoc networks[J]. Journal on Communications, 2010(5):1-9

[6] Amaresh M, Usha G. Efficient malicious detection for AODV in mobile ad-hoc network[C]// IEEE International Conference on Recent Trends in Information Technology(ICRTIT). Chennai, 2013:263-269

[7] Bhoi S K, Nayak R P, Dash D, et al. RRP: A robust routing protocol for Vehicular Ad Hoc Network against hole generation attack[C]// IEEE International Conference on Communications and Signal Processing (ICCSP). Melmaruvathur, 2013: 1175-1179

[8] Bao F, Chen R, Chang M J, et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. IEEE Transactions on Network and Service Management, 2012, 9(2):169-183

[9] Josang A, Knapskog S J. A metric for trusted systems[C]// Proceeedings of the 21st National Security Conference. 1998:16-29

[10] 胡玲珑,潘巨龙,崔慧. 无线传感器网络中基于信誉的恶意节点检测方法[J]. 中国计量学院学报, 2012, 23(1):41-47
Hu Ling-long, Pan Ju-long, Cui Hui. A reputation-based method for detecting malicious nodes in WSNs[J]. Journal of China Jiliang University, 2012, 23(1):41-47

[11] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):318-328

[12] Jiang T, Baras J S. Trust Evaluation in Anarchy: A Case Study on Autonomous Networks[C]// INFOCOM. Barcelona, Spain, 2006

[13] Ding Q, Li X, Jiang M, et al. Reputation-based trust model in vehicular ad hoc networks[C]// IEEE International Conference on Wireless Communications and Signal Processing (WCSP). Suzhou, 2010:1-6

[14] Saraswat D, Chaurasia B K. AHP Based Trust Model in VANETs [C]// 2013 5th International Conference on Computational Intelligence and Communication Networks (CICN). Mathura, 2013:391-393

[15] 田俊峰,鲁玉臻,李宁. 基于推荐的信任链管理模型[J]. 通信学报, 2011, 32(10):1-9
Tian Jun-feng, Lu Yu-zhen, Li Ning. Trust chain management model based on recommendation[J]. Journal on Communications, 2011, 32(10):1-9

[16] Mui L. Computational models of trust and reputation: Agents, evolutionary games, and social networks[D]. Cambridge: Massachusetts Institute of Technology, 2002

[17] Dellarocas C. Reputation mechanism design in online trading environments with pure moral hazard[J]. Information Systems Research, 2005, 16(2):209-230

[18] 王良民,郭渊博,詹永照. 容忍入侵的无线传感器网络模糊信任评估模型[J]. 通信学报, 2010, 31(12):37-44
Wang Liang-min, Guo Yuan-bo, Zhan Yong-zhao. Fuzzy trust model for wireless sensor networks with intrusion tolerance[J]. Journal on Communications, 2010, 31(12):37-44