MANET中基于声誉机制的安全路由协议

谭长庚，戴小村，王建新
（中南大学 信息科学与工程学院，湖南 长沙 410083）

摘 要：移动自组网是一种特殊的对等式网络，由于拓扑动态变化、无线信道完全开放、没有固定基础设施等特性，易遭受各种攻击，因此移动自组网的安全性显得尤其重要。在分析现有安全路由协议的基础上，设计了一种由节点直接声誉值和间接声誉值组成的声誉评价机制，对于间接声誉值更注重于由近期的交互所获得的声誉值。并在此基础上提出了安全路由协议SR－DSR，选择路径声誉值与路径长度比值最大的路由来发送数据包，提高了数据包传输的可靠度。通过仿真实验表明，在网络遭受恶意节点攻击时，SR－DSR比DSR在包到达率和网络吞吐量方面具有更好的性能。

关键词：移动自组网；声誉机制；安全路由协议
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1673－629X(2010)11－0162－04

A Security Routing Protocol Based on Reputation Mechanism in MANET

TAN Chang-geng, DAI Xiao-cun, WANG Jian-xin
(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: Mobile Ad hoc network is a special peer－to－peer network. Because of dynamic topology, openness of wireless channels, infrastructureless, it is vulnerable to various attacks, so the security issue is very essential to Ad hoc networks. Based on analysis of the existing security routing protocol, design a reputation evaluation mechanism, which composed of node's direct reputation value and indirect reputation value. However, for indirect reputation value, focus on the value obtained by the recent interaction. And last exploit a security routing protocol, called it SR－DSR. In this protocol select a path with largest value, the path reputation ratio of the length of the route to send the packets, to improve the reliability of packet's transmission. The simulation results show that SR－DSR protocol can get better performance in packet delivery ratio and throughput while there are attacking nodes in networks.

Key words: mobile Ad hoc networks; reputation mechanism; security routing protocol

0 引 言

移动自组网(Mobile Ad hoc Networks)是由一组带有无线收发装置的移动节点组成的无线移动通信网络，是一种不需要依靠现有固定通信网络基础设施的、没有任何中心实体的、自组织自愈的网络。网络中的各个节点相互协作、通过无线链路进行通信、交换信息，实现信息和服务的共享。移动自组网的安全目标与传统的有线网路中的安全目标是一致的，需要考虑以下安全属性：实用性、机密性、完整性、安全认证和非否定性。由于移动自组网络的特殊性，使得实现这些目标时面临诸多的挑战[1,2]。

由于使用无线信道、有限电源、分布式控制等原因，移动自组网比有线网络更容易受到被动窃听、主动篡改、信息假冒等各种方式的攻击。因为网络节点的能源有限，CPU的处理能力较低，所以很难实现复杂的加密算法，增加了信息被窃听的可能性[3]。加之节点的移动性，网路的拓扑和成员不断变化，节点间的信任关系也处在动态的变化当中，因此只具有静态配置的安全方案在移动自组网中是不可行的。与加密性算法相比，基于声誉机制的合作性方案既可以建立节点间良好的信任关系，又能节省一定的网络资源[4,5]。

收稿日期：2010－03－04；**修回日期**：2010－06－15
基金项目：国家自然科学基金(60873265,60903222)
作者简介：谭长庚(1963－)，男，博士，副教授，CCF会员，研究方向为移动自组网的路由协议和性能评价。

1 相关的研究工作

移动自组网的路由安全问题是目前的研究热点，已经有很多学者在相关领域取得一定的研究成果。

文献[6,7]提出了针对不良节点攻击的一种基于DSR协议的反应式链路协议：CONFIDANT。该协议主要包括以下组件：Monitor用于检测节点行为；Trust Manager用于控制发送、接收警告信息的情况；Reputation System用于记录和管理声誉信息；Path Manager使节点根据声誉记录情况对路由选择做出调整。仿真

实验表明在网络中存在一半的攻击节点时,该协议也具有较好的性能。

Core[8]针对节点的不良行为和自私行为提出了一种联合声誉机制,该机制拥有一个 Watchdog,另外还有一个完善的声誉机制,包括:Subjective Reputation(由观察者提出),Indirect Reputation(由其他节点报告得到),以及 Functional Reputation(特殊任务行为)。这些行为联合起来决定其节点的声誉值。以便来决定与该节点继续通信还是逐渐隔离。协议注重节点历史行为,采用既惩罚又奖励的策略,但是声誉值的传输得不到保障。

文献[9]在声誉值系统中引入了 time 和 context 两个因子,提出了一种增强的声誉机制模型,实验表明,该机制能有效区别声誉值的虚假推荐和诚实推荐,从而能可靠地防止节点合谋和诬陷攻击。

文献[10]中作者依据节点的声誉值来激励节点的合作行为和处罚节点的不合作行为,在该信任模型中,节点只根据本地的信息来评估其它节点的声誉值。

文献[11]提出了一种 LeakDetector 机制,用于解决 Ad hoc 网络中邻居节点合谋隐瞒丢包的问题,并弥补了现有安全路由协议只能监测一跳邻居行为的缺陷。LeakDetector 机制能够有效解决带有类似于 watchdog 监测器的路由协议无法检测节点合谋掩饰丢包的情况。不过,此方案需要周期性地更新虚拟图信息,使得节点开销较大,容易缩短网络寿命,不适合拓扑结构复杂的网络。

研究者们根据移动自组网的不同应用提出了不同的安全解决方案,但是现有的关于移动自组网的安全问题的研究具有一定的局限性,大多只是考虑单个节点的恶意行为对网络造成的破坏,而对网络中出现多个节点合谋攻击的情况则研究的较少,文中首先提出了一个声誉机制模型,然后在该机制上基于 DSR 提出了一种安全路由协议 SR-DSR。通过仿真实验证明,当网络中存在恶意节点时,该协议在包到达率和吞吐量方面较 DSR 有更好的性能。

2　声誉机制评价模型

针对移动自组网络的特点,建立无中心节点的分布式的声誉评价机制,节点打开监控模式,通过监控获得邻居节点的信息。当节点有数据包要发送给下一跳邻居节点时,先缓存数据包后再发送给下一跳邻居节点并监控其行为,监控周期为 $\triangle T$。节点在缓存数据包的同时还要执行另一个操作,就是在声誉值表中使记录与被监视节点在监控周期内交互次数的计数器 actnums 加 1。此外在数据包发送节点的邻居域中的其他节点侦听到数据包后,则判断数据包的接收节点是否为自己的邻居节点。若是,则缓存数据包,且执行与数据包发送节点相同的操作,但不转发数据包;若不是则丢弃数据包,不执行任何操作。在监控周期内,当节点每监控到下一跳节点成功转发一次数据包时,则在缓存中删除相应的缓存包,并在声誉值表中使记录与被监视节点在监控周期内成功交互次数的计数器 sucnums 增 1。

2.1　节点声誉值的计算

每个节点都有一个声誉值链表,保存本节点对其他节点的声誉评价。声誉值链表中的数据项如下:

nodeId	repval	actnums	sucnums	totalactnums	totalsucnums	lasttime

nodeId 为节点 ID;repval 为节点的声誉值;actnums 为节点在监控周期内的交互次数;sucnums 为节点在监控周期内的成功交互次数;totalactnums 为节点交互总次数;totalsucnums 为节点成功交互的总数;lasttime 为节点最近一次交互的时间。在 ΔT 内,若节点的丢包率 p_{drop} 大于阈值 DROP_THRESHOLD,则节点的声誉值就按公式(1)计算;若丢包率小于阈值,则节点的声誉值由公式(2)计算。

$$repval = repval - SUB\_VAL \tag{1}$$

$$repval = repval + ADD\_VAL * (1 - p_{drop}) \tag{2}$$

其中 $p_{drop} = 1 - \frac{sucnums}{actnums}$,一般情况下对节点的惩罚力度大于奖励力度,使节点的信誉建立难、失掉容易,因此 SUB_VAL 的值要适当大于 ADD_VAL。节点的声誉值计算完毕后,应执行公式(3)和公式(4)的操作,并把 actnums 和 sucnums 清 0,以免累积到下一个监控周期。

$$totalactnums = totalactnums + actnums \tag{3}$$

$$totalsucnums = totalsucnums + sucnums \tag{4}$$

节点声誉值的有效范围为 0 到 1,若出现节点的声誉值大于 1,则把声誉值置为 1,同理若声誉值小于 0,则把声誉值置为 0。

2.2　声誉值的更新

节点的声誉值更新一般有触发式更新和周期性更新两种方法[12],文中采用周期性更新声誉值,节点每隔一定时间就广播声誉值表中节点的声誉值信息,当节点接收到该声誉值信息时,首先检查广播信息的节点是否可信,可信就接收该声誉值信息,否则就丢弃该声誉信息。节点收到声誉信息后按照下面的公式进行声誉值的更新。

$$R_a(b) = \alpha R'_a(b) + (1 - \alpha) N_a(b) \tag{5}$$

$$N_a(b) = \frac{\sum_{j \in K_a} R_a(j) T_j(b) / (2^{n_j - 1})}{\sum_{j \in K_a} R_a(j) T_j(b)} \tag{6}$$

$R_a(b)$ 表示节点 a 对节点 b 的声誉值，$R'_a(b)$ 为当前声誉值，$N_a(b)$ 为 a 的邻居中可信节点集合 K_a 中节点对 b 的声誉值评价结果，α 表示声誉值的权重因子，$T_j(b)$ 为 j 传递过来的对 b 的声誉值。n_j 表示节点 j 与 b 最近一次交互的时间到 j 广播声誉值信息时所经历的周期数。由公式(7)得到：

$$n_j = \text{ceil}((T'_j - T''_j)/T_3) + 1 \tag{7}$$

T'_j 为 j 广播声誉值信息的时间，T''_j 为 j 与 b 最近一次交互的时间，T_3 为声誉值更新周期。ceil(x) 表示对 x 下取整。对节点 j 广播过来的声誉值更偏重由近期的交互获得的声誉值。这样可以防止一些恶意节点刚进入网络时表现良好，当获得较高的声誉值时就开始破坏网络。比如广播虚假的声誉值信息，恶意抬高或降低某些节点的声誉值。

3 基于声誉机制的安全路由协议 SR－DSR

文中在原路由协议 DSR 的基础上加入了声誉机制，并由此提出了基于声誉机制的安全路由协议 SR－DSR。

SR－DSR 协议是在 DSR 协议的基础上进行改进的。其原理大致如下：源节点若要与目的节点进行通信，首先检查路由缓存中是否有到目的节点的路径，如果有，则从路径中选择同时满足下面两个条件的路径来发送数据：

(1) 所选路径中不存在声誉值低于阈值 REP_THRESHOLD 的节点(声誉值低于阈值则被认为是恶意节点)；

(2) 所选路径的 w 值是路由缓存中到目的节点路径中最大的；w 值由公式(8)计算而得，是一个路由选择的安全可靠尺度。

$$w_i = \frac{\text{minrep}(\text{path}[i])}{\text{hops}(\text{path}[i])} \tag{8}$$

minrep(path[i]) 得到路径 i 的声誉值，即等于该路径上声誉值最小的节点的声誉值；hops(path[i]) 得到路径 i 的跳数。

若源节点缓存中没有到达目的节点的路径，则初始化 RREQ，进行路由发现。中间节点收到 RREQ 时，首先检查自己的路由缓存中是否有到目的节点的路径，如果存在，则同样根据上述条件(1)和(2)来判断路径是否合适，若存在合适的路径则发送 RREP 到源节点。若不存在合适的路径则把自己的地址加入到 RREQ 中，并继续广播 RREQ 直到目的节点。目的节点收到 RREQ 时，则发送 RREP 到源节点。中间节点只转发那些可信节点的 RREQ 包和 RREP 包。如果不可信，则丢弃该包。源节点收到多个 RREP 后通过条件(1)、(2)选择合适的路径发送数据。如果源节点多次重发 RREQ 并经过一段时间没有收到 RREP 时，则放弃路由发现，寻路失败。

在数据包抢救阶段，抢救数据包的节点也要根据上述条件来查看自己的缓存是否有合适的路径到目的节点，若没有则放弃数据包的抢救，只发送 RERR 到源节点表示路径断裂，数据传输失败。若有则抢救数据包。

在数据包的传输过程中，监控节点根据监控的信息对被监控节点的声誉值进行更新，若发现其声誉值低于阈值则认为被监控节点为恶意节点，监控节点不再把数据包发送给被监控节点，而是查看自己的路由表中有无合适的路径到目的节点，若有则重新选择一条路径发送数据到目的节点，若无则缓存数据包，执行寻路操作。并发送 ALARM 警告信息到源节点，ALARM 中包含恶意节点的地址，收到 ALARM 的中间节点则把恶意节点加入到自己的黑名单中并删除节点本身路由缓存中到恶意节点的路径。源节点收到该信息后则也执行同样的操作，并重新选择合适的路径发送数据包到目的节点。

因只转发可信节点的 RREQ 和 RREP，故整个网络中 RREQ 和 RREP 包总数目会相对减少。

4 仿真环境和仿真结果分析

4.1 仿真工具和性能参数

文中使用 Glomosim 2.03 来仿真协议的性能。Glomosim 是由加州大学洛杉矶分校 UCLA(University of California in Los Angeles)开发的基于 Parsec 并行执行的环境的并行可扩展离散事件仿真环境，非常适合对大型无线移动网络进行仿真。

在 2000 * 2000 的区域内随机布置 50 个节点，其中 10% 的恶意节点。仿真时间为 1000s，节点使用 Random Waypoint 移动模型，以 0～20m/s 的速度运动。通信模型采用 CBR 流，CBR 流大小为 512 字节，每秒钟发 10 个数据包，从源节点到目的节点有不间断的数据包发送。每个场景进行 10 次随机试验，每次试验采用 6 组 CBR 流，然后取平均值。

网络中恶意节点的攻击模型：

(1)恶意节点不发送数据包，不发送路由请求；

(2)恶意节点转发所有的路由请求包和路由回复包；

(3)恶意节点不进行任何数据包抢救；

(4)在某个通信区域内，如果只有单独的恶意节点，则恶意节点对收到的数据包采取全部丢弃，并诬陷其他的正常节点；若存在两个或两个以上的恶意节点，

则路由中的上游节点不丢包,下游节点丢弃所有的数据包,上游恶意节点掩护下游节点的丢包行为,并共同恶意诬陷其他正常节点。

为了比较 DSR 和 SR－DSR 协议在网络中存在恶意节点攻击下的性能,定义了以下的性能指标:

(1)包到达率(Packet Delivery Ratio):网络中所有目的节点收到包与所有源节点发送包的比率;

(2)吞吐量(Throughput):单位时间内应用层中所有目的节点吞吐量之和;

(3)网络控制开销(Ctrl Cost):网络中控制包数目除以数据包与控制包之和。

4.2　仿真结果与性能分析

为了表示方便,以下所有图中用 DSR 表示加入攻击节点的 DSR 协议的性能曲线,SR－DSR 表示加入攻击节点的安全路由协议 SR－DSR 的性能曲线。

从图 1 中可以看出在 DSR 中加入攻击节点后,数据包的到达率几乎为 50%,但是随着节点停留时间的增加,网络中的包的到达率有了些许的提高,这是因为随着停留时间的增加,网络中的节点处于一种相对静止状态,从而减少了恶意节点破坏网络的范围,因此使得包的到达率有了一点提高。SR－DSR 协议则使包的到达率得到了较大的提高,接近于 90%,不过随着节点停留时间的增加,包的到达率有一些下降,这是因为停留时间增加后,节点的移动性减小,节点间交互信息的速度减慢,对恶意节点的检测效率就会降低,从而引起了包的到达率的降低。

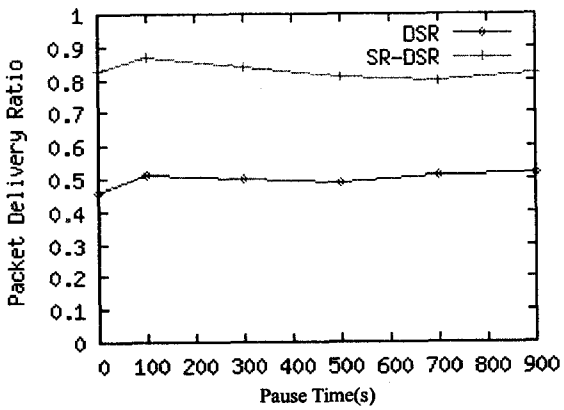

图 1　DSR 与 SR－DSR 包到达率比较

从图 2 中可以看出 SR－DSR 协议在网络吞吐量方面较 DSR 也有了较大的提高,不过随着节点停留时间的增加,DSR 的吞吐量有增加的趋势,SR－DSR 则表现出下降的趋势,这是因为在 SR－DSR 中网络的控制开销随着停留时间的增加而相应变大,挤占了网络的带宽,因此吞吐量有所减小。

从图 3 可知,SR－DSR 协议中,网络的开销有了一定的提高,并随着停留时间的增加有提高的趋势,这可能是因为 SR－DSR 中增加了对恶意节点的检测控制开销,随着网络拓扑趋于稳定,导致某些区域通信较密集,相应增加了路由错误包的数目,因此网络开销略有增大。而在 DSR 协议中,恶意节点直接丢包,使得网络中传输的数据包减少,从而减少了对数据包的抢救开销,并且随着停留时间的增加,网络趋于稳定,路由发现和路由回复包的数目相对减少,因此通信代价有下降的趋势。

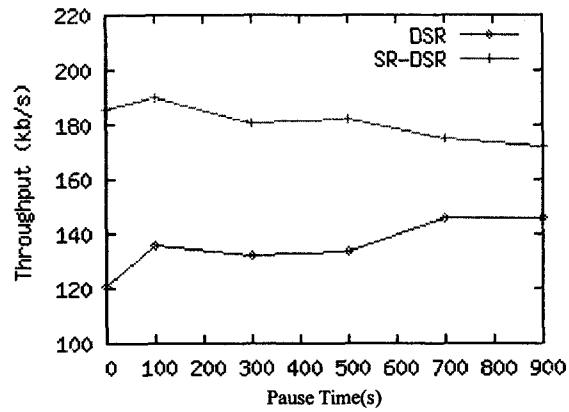

图 2　DSR 与 SR－DSR 吞吐量的比较

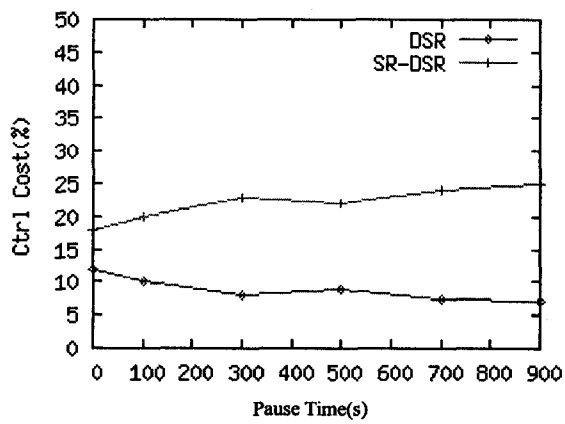

图 3　DSR 与 SR－DSR 网络控制开销比较

5　结束语

文中分析了移动自组网络的特点以及存在的安全隐患,并在现有针对网络攻击的主要防御机制的基础上提出了一种声誉机制防御模型,以提高网络中包的到达率。该声誉机制采用路由中上游节点和该节点的满足一定条件的直接邻居共同对路由中的下游节点进行监视,这样既可以降低节点的误判率,而且也能有效地防御节点的合谋攻击。同时在声誉值更新时对节点传递过来的声誉评价,根据与被评判节点最近的交互时间对传递的声誉值赋予不同的权值,使声誉评价更合理。

(下转第 169 页)

张车牌图像(图像分辨率、颜色背景等各不相同),实验中能准确定位 92 张图像,平均处理时间为 105ms,准确率达 92%,证明所使用的算法具有实时性和鲁棒性。试验利用 MATLAB7.0 进行仿真实验,运行在 P4/2.0GHz,512M 内存的 PC 环境中。

4　结束语

文中使用数学形态学对原始车牌图像进行了预处理,得到了较好的处理效果,并且通过阈值分割的迭代算法,得到的阈值准确率高,为进一步进行车牌识别提供了很好的效果。数学形态学运算也具有滤波作用,进一步去除了图像的噪声,形态学边缘检测相对于边缘检测算子具有算法简单、速度快、定位准确和抗干扰能力强的优点。通过对不同车牌图像进行试验,算法具有较好的识别结果。但是对于车牌倾斜情况下得到的图片,处理效果不明显,算法还有待进一步改进。

参考文献:

[1] 李　丰.车牌自动识别系统中的牌照区域图像分割技术[J].河南教育学院学报,2009,18(3):32-34.

[2] 黄明蕾.车牌识别系统中图像分割与识别技术研究[J].科技创业月刊,2007(3):189-190.

[3] 赵俊梅,张利平.基于数学形态学的车牌识别方法[J].车辆与动力技术,2008(4):31-34.

[4] 周宏强.基于小波—形态学的车牌图像分割算法[J].电脑编程技巧与实现,2009(3):92-93.

[5] Parker J R, Federl P. An Approach to Licence Plate Recognition[J]. IEEE Transactions on Industrial Electronics, 2000, 47(1):17-23.

[6] Zheng Danian, Zhao Yannan, Wang Jiaxin. An Efficient Method of License Plate Location[J]. Pattern Recognition Letters, 2005(26):2431-2438.

[7] 邹　星.车牌识别中的图像提取与分割算法[J].重庆工学院学报(自然科学),2009,23(8):19-23.

[8] Sauvola J, Pietikainen M. Adaptive document image binarization[J]. Pattern Recognition, 2000(33):225-236.

[9] 陈利娟,徐利华.消噪和数学形态学结合的字符图像预处理算法[J].现代电子技术,2009(3):110-118.

[10] 廖　明,张金林,甄树新,等.一种实用车牌定位算法及实现[J].系统仿真学报,2005,17(10):2349-2357.

[11] 高洪波,王卫星.一种二值图像连通区域标记的新算法[J].计算机应用,2007,27(11):2776-2784.

[12] 杜培明,陈　亮,赵玉贵.车牌字符分割与识别算法的研究与实现[J].仪器仪表用户,2009,16(1):17-19.

[13] Anagnostopoulos C N, Anagnostopoulos I, Loumos V, et al. A license plate recognition algorithm for intelligent transportation system applications[J]. Traffic Technology International, 2005(5):1-16.

(上接第 165 页)

在该声誉评价机制和 DSR 协议的基础上,文中提出了一种新的安全路由协议 SR-DSR,根据仿真实验,在网络中存在恶意节点的情况下,SR-DSR 比 DSR 在包到达率和网络吞吐量方面都有明显提高。

参考文献:

[1] 谭长庚,陈松乔,王建新.移动自组网中一种优化的局部声誉系统[J].计算机工程与应用,2008, 44(9):20-23.

[2] 李金鹏,吕光宏,王立军,等.移动 Ad Hoc 网络安全路由协议研究[J].计算机技术与发展,2008,18(7):24-28.

[3] 谭长庚,李　江.移动自组网中基于推荐的信任模型[J].计算机技术与发展,2009,19(11):68-71.

[4] 谭长庚,罗文燕,陈松乔,等.移动 Ad hoc 网络中节点合作性研究综述[J].计算机科学,2007,34(4):24-27.

[5] 荆　琦,唐礼勇,陈　钟.无线传感器网络中的信任管理[J].软件学报,2008,19(7):1716-1730.

[6] Buchegger S, Le Boudec Jean-Yves. Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks[C]// Proc. of IEEE, ACM Workshop on Mobile Ad Hoc Networking and Computing(MOBIHOC2002). EPFL, Lanusanne, Switzerland: [s.n], 2002:226-236.

[7] Buchegger S, Le Boudec Jean-Yves. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks[C]// Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. [s.l.]: [s.n.], 2002:403-410.

[8] Michiardi P, Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks[C]// Sixth IFIP Conference on Security Communications and Multimedia(CMS2002). Portoroz, Slovenia: [s.n.], 2002:107-121.

[9] Liu Jinshan, Issarny V. Enhanced Reputation Mechanism for Mobile Ad hoc Networks[C]// In Proc. of iTrust. Oxford, UK: [s.n.], 2004.

[10] He Q, Wu D, Khosla P. A secure incentive architecture for ad hoc networks[J]. Wireless Communication Mobile Computing, 2006, 6(3):333-346.

[11] Mogre, Hollick M, Steinmetz R. Detection of colluding misbehaving nodes in mobile Ad Hoc and wireless mesh networks [C]. [s.l.]: [s.n.], 2007:5097-5101.

[12] 王建新,张亚男,王伟平,等.移动自组网中基于声誉机制的安全路由协议设计与分析[J].电子学报,2005, 33(4):596-601.