无线自组织网络高准确度自私节点检测机制

杜君[1]，李伟华[1]，张克旺[2]，蒋卫华[3]
（1.西北工业大学计算机学院，710072，西安；2.西安交通大学电子与信息工程学院，710049，西安；
3.中国民航局航空安全技术中心，100028，北京）

摘要：针对现有自私节点检测机制无法对自私节点和失效节点进行准确区分，且自私节点误检率高的缺点，提出了一种高精确度自私节点检测机制(ASD).该机制基于无线设备接收数据需要满足一定信噪比要求以及自组织网络中节点分布密集的特点，选择具有更高信噪比的临近节点作为检测代理对转发节点进行检测，在提高检测精度的同时对网络中的失效节点和2种不同类型的自私节点进行准确区分.在ASD机制下，当节点发送自身数据而不转发临近节点的数据时，该节点被判断为自私节点，从而可实现自私节点与失效节点的区分；当节点对临近节点数据拒绝转发而仍然对临近节点进行确认应答(ACK)响应时，该节点被判断为拒绝转发节点，进而可实现拒绝转发自私节点与拒绝ACK响应自私节点的区分.仿真结果表明，ASD机制在任意拓扑结构下的自私节点误检率降低了31%，平均检测精度提高了12%.

关键词：无线自组织网络；自私节点检测；信噪比；检测精度
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2010)08-0025-05

An Accurate Detection Scheme for Selfish Nodes in Wireless Ad Hoc Networks

DU Jun[1]，LI Weihua[1]，ZHANG Kewang[2]，JIANG Weihua[3]
(1. School of Computer，Northwestern Polytechincal University，Xi′an 710072，China；2. School of Electronics and Information Engineering，Xi′an Jiaotong University，Xi′an 710049，China；3. Research Center of Security Technology，Civil Aviation Administration of China，Beijing 100028，China)

Abstract：Existing detection schemes for selfish nodes are inefficient since they can not distinguish selfish nodes from faulty nodes accurately and the false detection rates of these schemes are high. A novel detection scheme for selfish nodes named accurate selfish node detection (ASD) is proposed. The scheme uses SINR model of wireless transceivers，and is based on the character that ad hoc networks are usually densely deployed. Nodes with higher SINR are selected as agents to monitor the relay nodes so that selfish nodes can be detected precisely and can be distinguished from faulty nodes accurately. Based on the facts that selfish nodes send their own packets but deny to relay packets from its neighboring nodes and that faulty nodes never transmit their own packets the ASD is able to distinguish selfish nodes from faulty nodes. There are two types of selfish nodes，some selfish nodes deny to forward data packets，while others deny to reply acknowledgement packets to its neighboring nodes. The ASD can distinguish these two types of selfish nodes precisely. Simulation results and comparisons with the existing detection schemes show that the average false detection rate is reduced by 31% and the average accuracy of detection is raised by 12%.

Keywords：Ad Hoc network；selfish node detection；signal to noise ratio；detection accuracy

无线自组织网络具有自组织、自恢复的特点，在军事、救灾、临时会议等领域具有广阔的应用前

收稿日期：2010-01-08. 作者简介：杜君(1979—)，男，博士生；李伟华(联系人)，男，教授，博士生导师. 基金项目：国家“863计划”资助项目(2006AA01Z406)；国家科技支撑计划资助项目(2008BAH37B04).

景[1]. 受节点体积的限制,无线自组织网络节点的能量、存储空间、运算能力等有限,为保护有限的能量或者资源,部分节点可能对临近节点要求转发的数据包不进行转发,从而造成自私节点问题[2]. 由于自私节点对临近节点请求转发的数据包直接丢弃,这样将引起介质访问控制(MAC)层、网络层甚至传输层的重传或者路由重选过程,对网络吞吐量造成严重影响. 网络中自私节点的检测、隔离技术是自组织网络性能优化与安全领域的重要研究方向,也是该领域的研究难点之一[3].

本文提出一种可靠的无线自组织网络自私节点检测机制,依据临近节点的信号强度以及无线设备接收数据的信噪比要求,将具有较强信噪比的节点被选择为检测节点,可极大降低误检率. 在某个节点的多个临近节点进行侦听监测的过程中,该节点是否为自私节点由多个节点通过选举产生,这样可进一步降低检测机制的误检率与漏检率,提高检测机制的检测精度.

1 系统模型

无线传播模型可以表达为[4]

$$P_r(A\rightarrow B)=G\frac{P_t}{d^{\lambda}},\ 2\leqslant\lambda\leqslant 4 \tag{1}$$

式中:$P_r(A\rightarrow B)$为节点 B 接收到节点 A 信号的强度;P_t 为节点 A 的发射功率;d 为节点 A 与节点 B 之间的距离;λ 是与传播环境相关的常数;G 为与节点无线收发器及工作频段相关的常数.

节点接收到的有效信号与噪声功率之比称之为信噪比,用 γ 表示. 只有当节点接收的信噪比大于某个值时,节点才能正确接收到消息. 节点 A 接收节点 B 发送的消息时,其信噪比可表示为

$$\gamma(B\rightarrow A)=10\lg\frac{P_r(B\rightarrow A)}{N_0} \tag{2}$$

式中:N_0 为环境噪声.

2 问题分析及新机制的提出

Marti 等人[5]提出的看门狗机制(Watch Dog, WD)具有较强的自私节点检测能力. 在该机制中,假设节点 S 通过中间 3 个节点 A、B、C 向节点 D 发送数据,节点 A 向节点 B 发送完数据后进行信道侦听,如果节点 A 侦听到节点 B 向节点 C 成功转发了该数据包,则认为节点 B 正常转发;如果没有侦听到节点 B 转发的数据包,则认为节点 B 存在自私行为. 由于 WD 机制针对临近节点转发的 DATA 消息进行监测,克服了端到端反馈机制[6]的不足,但该机制假设无线信道是对称的,即如果节点 B 能够成功接收节点 A 的数据,则节点 B 发送的数据同样能够被节点 A 接收. 然而,在现实环境中,受环境噪声以及节点间位置等因素的影响,无线信道往往是不对称的. 在节点 A 与节点 C 所处环境噪声不同的情况下,即使节点 C 可以成功接收数据,节点 A 也不一定能够成功接收节点 B 发送的数据,特别是在网络节点采用功率控制机制的情况下,节点 A 的发送功率可能大于节点 B 的发送功率,这样节点 A 侦听到节点 B 转发数据包的概率将急剧降低,该机制检测自私节点的误检率较高[7]. WD 机制的第 2 个缺点是不能准确区分失效节点和自私节点. 自组织网络中部分节点由于负载过重或者硬件故障不能接收和发送数据,这类节点称为失效节点. 失效节点与自私节点的主要区别是自私节点不转发临近节点的数据,但自身需要发送数据,而失效节点既不转发临近节点的数据,也不发送数据.

如图 1 所示,节点 A 通过中继节点 B 向节点 C 发送数据. 依据 WD 机制过程,节点 A 向节点 B 发送 DATA 消息后,通过信道侦听方式监测节点 B 是否存在自私行为,由于节点 B 与节点 A 之间的距离较远,在节点 A 所受环境噪声以及其他干涉信号的强度较大时,可能节点 C 成功接收了节点 B 的数据,而节点 A 无法正确接收节点 B 发送的数据,引起误判. 假设无线设备的信噪比要求为 β,依据式(2),在$\frac{P_r(B\rightarrow A)}{10^{\beta/10}}<N_0<\frac{P_r(B\rightarrow C)}{10^{\beta/10}}$的情况下,节点 C 可正确接收消息,而节点 A 不能正确接收消息.

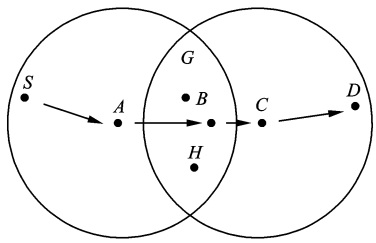

图 1 WD 机制在功率控制机制下的缺陷

在节点采用功率控制机制的情况下,由于节点 B 与节点 C 之间的距离较小,为降低节点功耗,节点 B 可能采用较低的发射功率发送数据,这样即使环境噪声较小,仍然可能引起误判. 假设节点 B 的发射功率为 P_1,当$\frac{N_0}{G}10^{\beta/10}\cdot d^{\lambda}(B\rightarrow C)<P_1<$

$\frac{N_0}{G}10^{\beta/10}d^{\lambda}(B\rightarrow A)$时，依据式(1)与式(2)，节点 A 不能正确接收节点 B 发送的数据，而节点 C 可以正确接收节点 B 发送的数据.

分析现有机制可以发现，引起误判的主要原因是现有检测机制中检测节点与接收节点距离待检测节点的距离不同，而且检测节点与接收节点所处的地理位置不同，所受的干涉也可能不相同. 在监测节点接收到发送节点所发送信号的信噪比大于或者等于接收节点接收到发送节点发送信号的信噪比的情况下，可实现较为可靠的自私节点检测；反之，则会出现误判断. 为此，我们提出一种基于信噪比强度的自私节点检测机制，该机制的基本思想为：在 $\gamma(B\rightarrow A)\geqslant\gamma(B\rightarrow C)$的情况下，节点 A 可以通过侦听节点 B 转发数据的方法进行自私节点的检测；在 $\gamma(B\rightarrow A)<\gamma(B\rightarrow C)$情况下，节点 A 在临近节点中寻找满足条件$\gamma(B\rightarrow G)\geqslant\gamma(B\rightarrow C)$的节点 G 作为监测节点，由于节点 G 成功接收节点 B 数据包的概率高于节点 C 接收 B 数据包的概率，同时也高于节点 A 接收节点 B 数据包的概率，所以本文所提机制的误检概率得以降低.

3　ASD 协议

3.1　定义与假设

定义 1　自私节点：任意企图保护自身资源或者过多占用无线信道资源的节点均被认为是自私节点.

定义 2　检测发起节点：为防止自私节点拒绝转发数据包，要求对自私节点进行检测的节点.

定义 3　待检测节点：目前接收到数据包，被怀疑可能是自私节点的节点.

定义 4　检测代理：实际实施自私节点检测的节点.

3.2　协议过程描述

本文提出的可靠自私节点检测机制(Accurate Selfish-node Detection，ASD)以节点接收数据包的信噪比为基础，可对上述 2 类自私节点进行准确检测. 下面以图 1 所示拓扑结构为例对协议进行描述.

ASD 机制基于跨层设计的思想，依靠 MAC 层以及网络层的服务提供可靠的自私节点检测. 假设节点 MAC 层协议基于载波监听多点接入(CSMA)机制发送数据，需要发送数据的节点在等待信道空闲时发送数据(DATA)消息，接收节点在接收到 DATA 消息后以确认应答(ACK)消息进行确认，发送节点在接收到 ACK 消息后认为接收节点成功接收数据. ASD 自私节点检测机制的步骤如下.

(1)网络中所有节点在接收数据过程中统计每个临近节点的信号强度，同时计算本节点受环境噪声等的干涉. 假设节点 B 接收到临近节点 A 的信号强度为 $P_r(A\rightarrow B)$，同时节点 B 所受的平均噪声为 N_0，根据公式(2)可计算节点 B 接收节点 A 的信噪比 $\gamma(A\rightarrow B)$，同样可以得到 $\gamma(B\rightarrow C)$、$\gamma(B\rightarrow G)$、$\gamma(B\rightarrow A)$. 在非对称链路假设下 $\gamma(B\rightarrow A)\neq\gamma(A\rightarrow B)$.

(2)接收节点 C 将自身得到的 $B\rightarrow C$ 构造网络层数据包 M_{SINR} 向检测发起节点 A 发送.

(3)节点 A 接收到 M_{SINR} 消息，得到 $\gamma(B\rightarrow C)$，

if $\gamma(B\rightarrow C)<\gamma(B\rightarrow A)$ then

　节点 A 自身为检测节点；

　转至步骤(8)；

else if $\gamma(B\rightarrow C)>\gamma(B\rightarrow A)$ then

　转至步骤(4)；

endif

(4)节点 A 在 MAC 层广播请求消息(M_{req})，其中包含 $\gamma(B\rightarrow C)$，由于是 MAC 层广播，只有节点 A 的临近节点接收到 M_{req} 消息；

(5)临近节点 G 接收到 M_{req} 消息，

if $\gamma(B\rightarrow G)>\gamma(B\rightarrow C)$ then

　节点 G 被选择为检测代理；

　发送响应消息(M_{res})响应检测发起节点；

endif

(6)检测发起节点接收到 x 个 M_{res} 消息，

if $x>0$ then

　检测发起节点得到合适的检测代理；

else

　节点 A 自身为检测节点；

　转至步骤(8)；

endif

(7)每隔一定时间，节点 G 向节点 A 发送汇报消息 M_{rep}，汇报这段时间内的检测统计值，包括被检测节点 B 向节点 C 转发节点 A 的数据包个数.

(8)分两种情况对自私节点进行检测

if 节点 A 自身为检测节点 then

　节点 A 直接判定节点 B 是否为自私节点；

else

　节点 A 根据多个检测代理的汇报信息，判断节点 B 是否为自私节点；

endif.

3.3　ASD 协议特点

ASD 协议的主要特点是可对自私节点进行准

确可靠的检测,同时,可对2种自私节点进行区分. ASD协议的核心思想是通过接收到被检测节点的信号强度更强的代理节点对被检测节点进行检测,从而降低误检率,提高检测准确度. 在该机制中,当被检测节点在某一段时间既不发送自身数据,也不转发临近节点数据时,可以认为该节点处于失效状态;当该节点只发送自身数据,而不发送临近节点数据时,则认为该节点为自私节点;当检测发起节点及其临近节点在某段时间内没有收到被检测节点的数据包时,则认为该节点为失效节点,只需从路由表中去除该节点即可;当检测发起节点或者检测节点的临近节点接收到该节点发送的数据包而请求该节点转发的数据包没有得到ACK确认和转发时,则认为该节点为第一种自私节点;当检测发起节点收到ACK消息,而经过检测代理检测,被检测节点没有转发DATA消息时,则该节点为第2种自私节点.

3.4 协议可能面临的安全威胁及解决方法

首先,协议可能面临检测代理与被检测节点间的联合欺骗. 在网络中存在不可信节点的情况下,部分检测代理可能对检测节点进行欺骗. 检测发起节点的临近节点 H 可能与节点 B 进行联合欺骗. 在协议的第6步可能通过伪造 M_{rep} 对节点 B 的自私行为进行掩盖. 在节点稠密部署的情况下ASD机制可解决联合欺骗问题,ASD机制采用选举算法对这种联合欺骗行为进行处理,即在节点密集部署的情况下,节点 C 通过 M_{req} 消息可能获得多个检测代理,这多个检测代理发送的数据通过选举算法,可对联合欺骗节点的汇报结果进行否决,从而解决这种联合欺骗问题.

其次,在协议第2步,自私节点 B 可能对转发的 M_{SINR} 消息中包含的信噪比数据 $\gamma(B\rightarrow C)$ 进行修改. 这种修改的目的是为联合欺骗做准备. 例如,节点B通过修改 $\gamma(B\rightarrow C)$ 为某一较大值,这样由于 $\gamma(B\rightarrow C)>\gamma(B\rightarrow A)$,检测发起节点 A 发送 M_{req} 消息,节点 H 发送 M_{res} 消息成为唯一的检测代理,进行后续联合欺骗. 在ASD协议中,通过2种方法对这种欺骗行为进行处理. 第一种方法是通过其他路径路由 M_{SINR} 消息,即节点 A 向节点 C 路由 M_{SINR} 消息时,避免选择通过节点 B 的路径,这样可防止节点 B 对数据进行修改,这种方法较适宜节点密集分布的情况. 第2种方法是采用公钥/密钥方式对 M_{SINR} 消息进行加密,防止节点 B 识别和修改节点 C 向节点 A 发送的数据. 虽然第2种方法这样方式具有较广泛的适应性,但对节点的运算能力提出了较高的要求. 在协议的实现过程中可以融合2种方法,即当存在多条由节点 C 向节点 A 的路径时,通过多路径的方式路由 M_{SINR} 消息;当只存在一条路径时,采用 M_{SINR} 消息加密的方式.

4 实验与性能分析

本文采用NS-2(Network Simulator)离散事件模拟器来构建无线自组织网络的模拟环境,对ASD机制与现有机制进行仿真对比.

本文采用数据包的投递率作为网络性能的衡量参数. 在第1个仿真实验中,网络由100个节点组成,随机选择100个节点中的5个节点为发送节点,其对应的接收节点也随机选择产生. 随机选择20%的链路为非对称链路,对这些链路的某个方向添加或者减少10%~15%的传播损耗,从而形成随机非对称链路.

图2所示为静止情况下自私节点影响网络性能的仿真结果. WD机制对存在非对称链路或者节点采用功率控制机制的情况下,检测自私节点的误检率较高,随着自私节点的增多,网络的数据包投递率迅速降低. ASD机制在存在非对称链路或者节点采用功率控制机制时,仍然可以对自私节点进行较为准确的检测,网络的吞吐量受自私节点的影响较小,随着网络中自私节点的增多,网络的投递率降低较少. 通过对20次任意随机拓扑的实验数据取平均,可以得出ASD机制的误检率降低了31%,自私节点平均检测精度提高了12%.

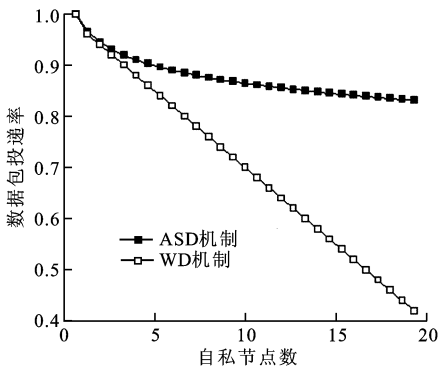

图2 静止情况下自私节点对网络性能的影响

第2个仿真实验对比了在不同节点移动速度情况下网络性能的变化情况. 仿真网络仍然由100个节点构成,随机选择5个发送节点和5个接收节点产生5个数据流,网络中自私节点为10个,随机选择产生. 节点运动模型采用Random Way Point运动模型.

图 3 所示为不同节点移动速度下网络性能的变化情况. ASD 机制中当检测发起节点、检测代理、被检测节点或者接收节点出现移动时，节点需要进行信号强度的检测，当满足一定条件时，需要发送数据包进行信息传递，M_{req}、M_{rep}等消息的交互会加重网络的负载. 在 ASD 机制中，节点的移动速度决定了信息传递的速率，最终影响这些协议负载对网络性能的影响. 从仿真结果中可以发现，当节点的移动速度大于 21 m/s 时，ASD 机制下的网络性能低于 WD 机制，但在常用自组织网络中，节点的移动速度远低于 21 m/s，因此 ASD 机制能够满足目前的实际应用.

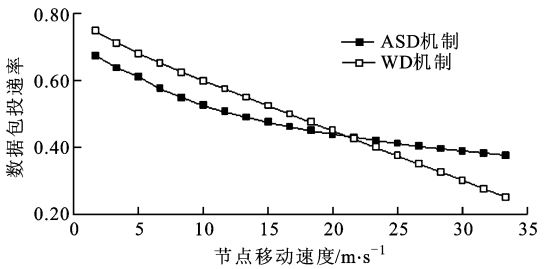

图 3　节点移动对检测机制的影响

最后，我们仿真在存在联合欺骗的情况下网络性能的变化情况. WD 机制完全依赖于检测发起节点对被检测节点的判断，因而不存在网络联合欺骗的情况. ASD 机制在一定情况下需要依靠检测代理对自私节点进行检测，而检测代理与检测发起节点间又可能存在一定的不可信关系，当检测代理与被检测节点存在联合欺骗时，可能造成节点的误检或者漏检，最终影响网络吞吐量. 图 4 所示为不同临近节点数的情况下数据包的投递率变化情况. 可以发现，在网络节点密度较大时（每个节点有 5.5 个临近节点），联合欺骗对网络的影响较小，ASD 机制比较适宜稠密部署的无线自组织网络.

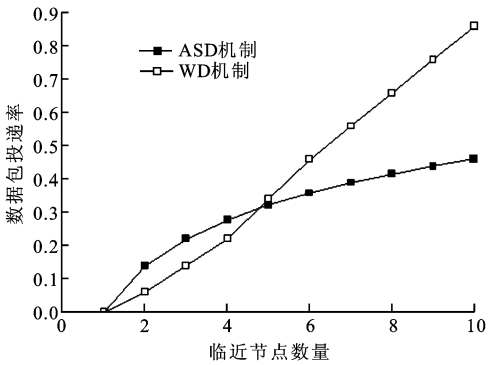

图 4　联合欺骗对网络性能的影响

5　结　论

自组织网络中自私节点引起网络各层的频繁重发，最终影响网络性能. 对自私节点进行有效的检测和隔离具有非常重要的意义，而准确高效的自私节点检测是实现自私节点隔离的基础. 本文提出的 ASD 机制是一种基于信噪比的自私节点检测机制，该机制借助于检测代理的方法，可显著提高自私节点检测的准确度，具有较高的实用价值.

参考文献：

[1] SU Hang, ZHANG Xi. Modeling throughput gain of network coding in multi-channel multi-radio wireless ad hoc networks [J]. IEEE Journal on Selected Areas in Communications, 2009, 27 (5): 593-605.

[2] LIU Chunfeng, SHU Yantai, LI Mingyuan, et al. Delay modeling and analysis of IEEE 802.11 DCF with selfish nodes [C]// Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing. Piscataway, NJ, USA: IEEE Press, 2008: 1-4.

[3] GUNASEKARAN R, RHYMEND UTHARIARAJ V, SUDHARSAN R, et al. Detection and prevention of selfish and misbehaving nodes at MAC layer in mobile ad hoc networks [C] // Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York, USA: ACM Press, 2008: 1945-1948.

[4] ANDREA G. Wireless communications [M]. New Jersey: Prentice Hall PTR, 2005.

[5] MARTI S, GIULI T J, LAI K, et al. Mitigating routing misbehavior in mobile ad hoc networks [C]// Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. New York, USA: ACM Press, 2000: 255-265.

[6] PAPADIMITRATOS P, HAAS Z J. Secure data transmission in mobile ad hoc networks [C]// Proceedings of the 2nd ACM Workshop of Wireless Security. New York, USA: ACM Press, 2003: 50-50.

[7] DJENOURI D, KHELLADI L, BADACHE A N. A survey of security issues in mobile ad hoc and sensor networks [J]. IEEE Communications Surveys & Tutorials, 2005, 7(4): 2-28.

（编辑　刘杨　苗凌）