Adhoc网络中节点的监控机制研究

Research of monitor-mechanism of node in Adhoc network

栗 帅，韩继红，王亚弟，陈 华

LI Shuai, HAN Ji-hong, WANG Ya-di, CHEN Hua

（信息工程大学 电子技术学院，郑州 450004）

摘 要：哪些节点能够监控，对节点的哪些行为进行监控，何时进行监控，什么样的信息进行举报等是监控机制应该考虑的问题。本文从分析自由监控机制、分级监控机制入手，基于分簇阶段的安全特点改进并设计了基于角色的分级监控机制。

关键词：Adhoc网络；监控机制；自由监控；分级监控；基于角色

中图分类号：TP393　　**文献标识码**：B　　**文章编号**：1009-0134(2010)02-0058-03

0 引言

Adhoc网络是一组无线移动节点组成的多跳的临时性的无基础设施支持的无中心网络。节点的监控主要是指在Adhoc网络中，节点之间依靠相互间的通信，将节点的行为情况进行反馈的一种通信机制。

节点间的监控机制在早些时候的信任管理相关文献中有记载，如自由监控在信任管理中比较普遍A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks有相关记载，后来由于考虑安全因素，出现了分级监控，如文献Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks中将节点间的监控分级，确保在监控阶段的安全。

1 相关研究

1.1 自由监控机制

在自由监控中相邻节点间可以相互监控，adhoc网络模型中通常都是这种模型。如图1所示。

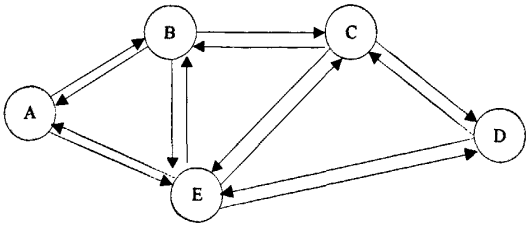
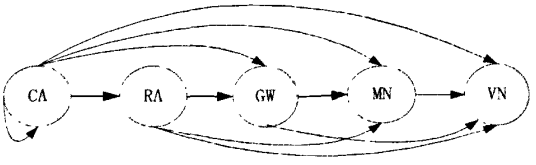


图1 自由监控模型

自由监控机制中，在跳数允许范围之内，节点可以互相监控。这些特性决定了自由监控模型对节点的约束性弱，只要能够直接通信的节点之间都能够相互监控。优点是节点间的监控能够及时全面，健壮性较好，但缺点是容易被恶意节点利用，通过虚假举报、恶意评估等手段，引起安全问题。

1.2 分级监控机制

分级监控主要解决的是节点的监控权力问题，即达到一定条件的节点才能对其他节点进行监控，降低节点间监控的随意性。下面是一种比较典型的分级监控模型，如图2所示。



CA为簇首 RA为注册中心 GW网关 MN为成员 VN为可疑

图2 分级监控模型

由于在有敌对节点的情况下，如果让信任度低的节点来监控簇首等信任等级高的节点则有安全隐患存在，本文提出了一种分级监控方式。节点分为五类：簇首(CA)，注册中心(RA)，网关节点(GW)，成员节点(MN)，游客节点(VN)。CA可以监控的状态节点为{CA，RA，GW，MN，VN}，RA的监控状态节点为{GW，MN，VN}，GW的监控状态节点为{MN，VN}，MN只能监控VN节点，VN节点不能监控任何节点。

1.3 监控机制分析

上述两种监控机制都是为解决某一问题而产生

收稿日期：2009-10-26

作者简介：栗 帅（1981－），男，河南登封人，硕士研究生，研究方向为计算机网络安全、信息系统安全。

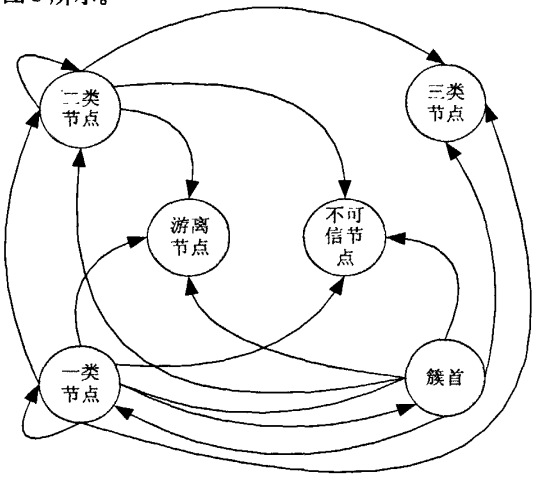
的，自由监控机制的发现时间有较大优势，而分级监控在控制节点的随意监控方面有较强优势。但在对安全性要求较高的场合，两种机制都显得力不从心。自由监控机制很容易被恶意节点所利用，造成节点间的恶意举报等行为发生，分级监控由于只允许特定节点进行单向监控，容易造成不能够及时发现节点间的恶意行为，使监控的可用性得不到应有的发挥。

2 基于身份的监控机制

2.1 监控模型

基于身份的监控模型将节点按照信任度分为五类：不可信节点，游离节点、三类簇内节点、二类簇内节点、一类簇内节点。

主要是利用二类簇内节点来监控整个网络的状况，也即二类簇内节点可以监控一类簇内节点，也可以监控三类簇内节点。而三类簇内节点则不具备监控权利，一类节点可以对其它节点进行监控。如图3所示。



→表示节点的监控

图3 基于身份的分级监控图

三类节点的监控报告可信度低，三类节点在簇内的比例小，形不成有效的效果；二类节点是簇内的中坚力量，也是可以信任的节点，能对簇首节点形成有效的钳制作用；一类节点能对所有簇内节点进行监控。这基本形成了分级监控，但由于三类节点占少数，也基本达到了相互监控的效果。

进行监控时，节点间定时进行信任的交互，即定期进行节点间信任表的相互发送，以达到节点信任列表的定时更新。监控的内容主要有：对节点行为的监控，对规定范围内节点的属性进行实时监控，发现有非正常现象及时处理报告。对节点的推荐信息及举报信息进行监控，推荐信息或者由簇首发起，或者定期进行，对符合条件的情况交由挑战响应模块进行处理。

在监控机制中，对节点的行为进行分类，引入策略库对不同的行为作出相应的处理。

2.2 监控对象

监控对象主要指基于一个节点在被动模式下能够收集关于其它节点的信息。如果在不同的协议层运用合适的方法通过分析接收，转发和偷听包等能够收集到重要的关于其它节点的信息。

//分析其他论文中关于监控对象的论述，再结合安全分簇算法的需求得出本文的监控对象。

根据安全分簇算法的安全需求，节点首先要在被动模式下可能的事件被测量和精确如表1所示。

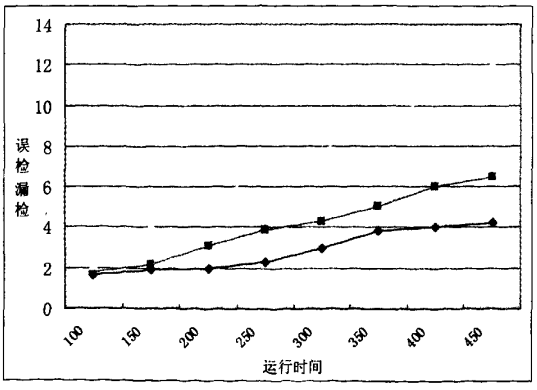
表1 定义数据格式

桢接收
数据包转发
控制包转发
数据包接收
控制包接收
流建立
数据转发
数据接收

3 性能分析

经证明，这样的监控方式在安全性、可用性、冗余性等方面比分级监控效果好。以下是假设3个簇共50个节点情况下作出的实验：

1）安全性，主要指标是漏检误检情况，与自由监控和分级监控相比发现恶意节点的时间和几率。



【下转第80页】

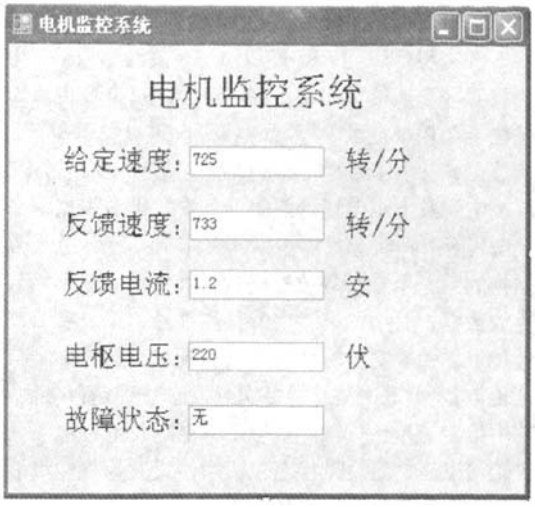


图3 上位机数据显示界面

这样上位机就收到某台电机此时的各种运行参数，由此可以实现使用上位机监控整个厂房中所有电机的运行状况。

在系统调试时，使用三米长的双绞线作为通信介质，上位机、直流电机、直流电机调速器等作为调试工具。实验证明，上位机能够顺利接收到直流电机发送的各种运行参数，说明系统已经实现了数据通信的要求。由于直流电机、测速机本身都是比较大的干扰源，在此情况下数据仍能顺利传输，这也一定程度上验证了CAN总线的抗干扰能力。

4 结束语

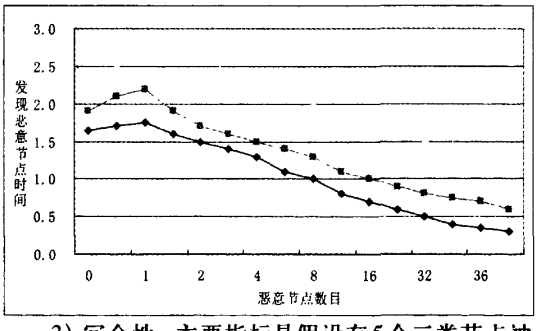
本文针对CAN总线在直流电机调速系统中的应用，通过整体结构设计，实现了直流电机调速器与CAN总线控制器之间的数据交换以及CAN总线与上位机间的数据传输，最终实现CAN总线对直流电机的运行状态的监视。

参考文献:

[1] 刘松,王渝.基于CAN总线的数字式直流电机控制系统[J].微计算机信息,2003,19(4):7-9.
[2] 曹太强,许建平,吴昊,王杰.基于DSP的直流电机数字调速系统的设计[J].电力电子技术,2008,42(2):73-77.
[3] 王田苗.嵌入式系统设计与实例开发[M].清华大学出版社,2002.
[4] 王泽民,芦东昕,谢鑫,徐立峰.基于VxWorks的异常处理的研究和实现[J].计算机工程,2005,31(13):90-92.
[5] 曹珊,于秀敏,周学文,等.混合动力汽车CAN总线系统智能节点设计[J].计算机工程与应用,2006,42(15):92-93.
[6] 王彦堂,李贻斌,宋锐.基于ARM Linux平台的CAN设备驱动程序设计与实现[J].计算机工程与应用.2007,43(15):79-82.

【上接第59页】

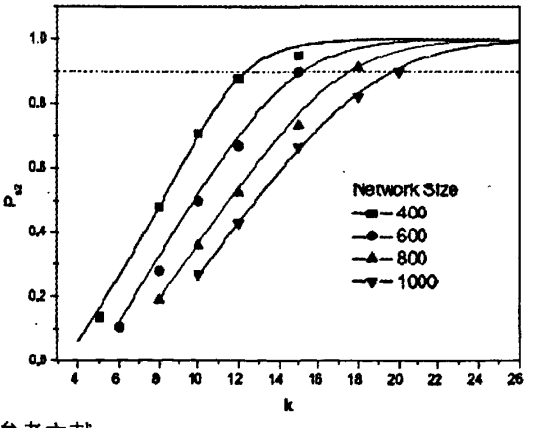
2) 可用性，主要指标是与自由监控和一般分级监控相比，恶意节点发现时间如何。



3) 冗余性，主要指标是假设有5个二类节点被俘虏对系统的影响。

4 结束语

A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks。



参考文献：

[1] Garth V.Crosby,2006,A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks,IEEE.
[2] Abderrezak Rachedi,2006,Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks,IEEE.
[3] Asad Amir Pirzada,2006,Establishing Trust in Pure Adhoc Networks.
[4] Zhaoyu Liu,2004,A dynamic trust model for mobile ad hoc networks,IEEE.

Adhoc网络中节点的监控机制研究

作者： 栗帅， 韩继红， 王亚弟， 陈华， LI Shuai， HAN Ji-hong， WANG Ya-di， CHEN Hua
作者单位： 信息工程大学电子技术学院,郑州,450004
刊名： 制造业自动化 ISTIC PKU
英文刊名： MANUFACTURING AUTOMATION
年，卷(期)： 2010，32(2)
被引用次数： 0次

参考文献(4条)

1. Garth V A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks 2006

2. Abderrezak Rachedi Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks 2006

3. Asad Amir Pirzada Establishing Trust in Pure Adhoc Networks 2006

4. Zhaoyu Liu A dynamic trust model for mobile ad hoc networks 2004

相似文献(2条)

1. 学位论文 张念丽 移动Ad Hoc网络的入侵检测系统研究 2007

近年来，移动AdHoc网络以其无需任何基础设施支持即可快速组网实现便捷通信的优异特性，已经获得各个领域的广泛关注。然而，由于其本身固有的介质开放、拓扑结构高速动态、缺乏集中监控机制、资源受限等特性，使得传统的用防火墙和加密软件来保护网络的做法已经不足以解决其安全问题，而在固定网络已经获得良好应用的入侵检测系统也很难适用于移动AdHoc网络。

本文在参考大量关于移动AdHoc网络、入侵检测技术和移动代理技术的基础上，提出了一种应用移动代理及临时分簇算法的移动AdHoc网络入侵检测系统MA-IDS，该系统在每个节点上设置入侵检测系统，实现本地检测。当某个节点发现入侵迹象而不能判定是否入侵时，就启用临时分簇算法对移动AdHoc网络进行分簇,然后由簇头完成多节点之间的协作检测。分簇使得MA-IDS系统抛弃了集中控制模式，实现了分布式检测和分布式控制，从而避免了单点失效现象，同时使该系统具有良好的扩展性。MA-IDS系统还引入了移动代理的概念，移动代理不仅能够减轻网络负载、缩短网络时延，而且具有异步自治执行以及动态自适应能力，使MA-IDS系统具有良好的性能。

最后针对MA-IDS系统，本文提出了一种新的分簇算法NWCA，该算法采用了组合加权的思想，更加全面地考虑了多种因素的影响，尤其考虑了安全因素的影响，以适应MA-IDS系统的需要。在MA-IDS中，NWCA是根据需要临时分簇，任务完成后，NWCA算法即结束。

2. 学位论文 程玉朋 基于移动Agent和分簇算法的无线ad-hoc网络分布式入侵检测系统研究 2006

无线AdHoc网络是由一组自主的无线节点相互合作而形成的一种独立于固定基础设施的自创造、自组织和自管理的网络。

由于无线通信链路的开放性、网络入侵手段的不断变化，使得AdHoc网络的安全问题越来越受到人们重视，无线AdHoc网络的安全问题也成为该领域研究的热点和难点。同传统的有线网络相比，无线AdHoc网络缺乏固定基础设施、没有集中控制点、分布式控制，导致传统的安全防护措施，如防火墙等被动网络安全技术在AdHoc网络中无法有效应用，而入侵检测系统作为一种主动式安全防护技术，弥补了传统安全技术的不足。但是，无线AdHoc网络的拓扑结构高度动态、采用分布式协作、节点网络带宽和节点电池容量受限、缺乏明确的防护线和集中监控机制，使得传统有线网络下的入侵检测技术在AdHoc网络环境下也不能直接应用。因此，需要研究新的适合无线AdHoc网络特性的入侵检测体系结构和检测方法。

移动Agent技术是近年来人工智能领域发展非常迅速的一种技术。由于移动Agent具有良好的自治性、主动性、交互性及可轻量级实现，在AdHoc入侵检测系统中有着非常好的应用价值。

本文首先对传统入侵检测技术和移动Agent技术进行了综述，然后针对AdHoc网络的特点设计了一个建立在网络分簇和簇头选择算法基础上的基于移动Agent的可生存性分布式入侵检测体系结构MABDIDS，在研究各种已有分簇算法的基础上对WCA(WeightClusteringAlgorithm)进行了改进，本文称之为KHAWCA，并在网络模拟器NS-2下对该算法进行了仿真实验。仿真结果表明，新提出的分簇算法能够提高网络中节点的最小生存时间和端对端吞吐量，取得了比较好的效果。