

MANET 入侵检测技术的研究

程 铃

(南京信息工程大学 电子与信息工程学院, 江苏 南京 210044)

摘 要: 移动自组网(MANET)是由移动节点自组织形成的无线网络,由于其动态拓扑的特点,容易遭受各种安全威胁,而入侵检测技术能有效地保障移动自组网的安全.对已有的分级入侵检测技术进行分析,提出一种基于区域分级的入侵检测系统(IDS),避免了对节点的重复监控及尺寸小的簇的形成,减少了节点的运算负荷与通信负荷,提高了簇头的稳定性,避免簇头频繁选举带来更多的资源消耗.

关键词: 移动自组网;入侵检测;区域;分级的入侵检测系统

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)06-0057-03

Study on Intrusion Detection for Mobile Ad Hoc Networks

CHENG Ling

(College of Electronic & Information Engineering, Nanjing University
of Information Science & Technology, Nanjing 210044, China)

Abstract: A mobile ad hoc network is a wireless network that is formed automatically by a collection of mobile nodes. It is particularly vulnerable due to its characteristics of dynamic changing topology. Intrusion detection technology can effectively protect mobile ad hoc networks from attack. In this paper, the existing hierarchical approach are analyzed and a zone-based hierarchical IDS is proposed. The new approach can prevent duplicate monitoring on nodes and small cluster fragments. Moreover, it can decrease the computational complexity and the bandwidth consumption, The stability of cluster heads is improved and resources consumption of cluster heads election is reduced.

Key words: mobile ad hoc network; intrusion detection; zone; hierarchical IDS

1 引言

移动自组织网(MANET)是由一组带有多跳的临时性的无线网络,它没有任何固定的基础设施和管理中心,彼此通信范围内的移动节点之间可以通过无线连接直接通信,而无线通信范围之外的节点则通过其他节点路由来进行消息转发.独特的网络特性和传输介质导致 MANET 存在诸多安全隐患,如节点间信任关系难以建立,路由依赖于节点的协作,数据易遭到窃听、重放或篡改,以及拒绝服务等.

为了保障 MANET 的安全,引入了入侵检测系统(IDS).IDS 能够帮助网络系统快速发现网络攻击的发生,扩展了系统管理员的安全管理能力(包括安

全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性^[1].入侵检测系统能实时监控系统活动,收集和分析监控数据,发现并报告违背安全策略的事件.入侵检测能够及时检测恶意攻击,制止攻击行为,减小进一步攻击带来的损失.

目前,传统有线网络的入侵检测技术的研究比较广泛,但是针对有线网络开发的入侵检测系统不适用于无线 Ad Hoc 网络.因此,急需开发一种新的入侵检测系统来保护无线 Ad Hoc 网络^[2].由于 MANET 具有动态拓扑、分布式协作、缺乏集中的监控、节点的带宽和计算能力有限等特征,给其 IDS 的设计带来了更多挑战,提出了更多的要求.具体为:(1)采用分布协作结构;(2)尽可能少用网络资源、节点能量和计算资源;(3)具有较低的误报率和

漏报率;(4)不依赖于路由协议;(5)不引入新的安全隐患.

2 分级 IDS

分级 IDS 是分布协作 IDS 的扩展,可用于多层的 MANET 系统中.已提出的分级 IDS 方案几乎都采用两级结构,网络划分成若干簇,每一簇中设一簇头,相邻簇共享一网关节点.簇头选择的标准:(1)一跳范围内节点(称为邻居节点)数目多;(2)簇成员都在簇头一跳范围内;(3)遭到攻击的概率小;(4)处理能力强、存储容量大、可用的能量充足.在分级 IDS 中,每个节点设有 IDS 代理,负责监控和检测本地入侵,簇头为簇内所有节点提供路由和支持安全措施,簇头监控网络分组,发现入侵时,启动全局响应.现已提出一些方案:

方案一:Kachirski O 和 Guha R 提出了基于移动 Agent 的入侵检测方案^[3].为了节省资源,只在某些节点上驻留监视网络的 Agent,并且 Agent 的数量可按要求进行增减.

方案二:Huang Y 和 Lee W 提出建立集团,每一集团即一跳范围内节点的集合,类似簇^[4];从安全出发,集团中随机选取簇头,因而所有的节点都有机会成为簇头.该方案不易遭受单点攻击,但由于随机选择簇头,可能出现较多的簇头,或选举的簇头能量匮乏而导致簇头频繁选举,消耗网络更多的计算和带宽资源.

方案三:Sterne D 等提出了一种动态的分级入侵检测方案^[5],每一节点都有监控功能,对检测到入侵检测进行响应,报警并报告上一级簇头,簇头对簇内成员节点送来的数据进行聚集和相关运算,并上报上级簇头.上级簇头管理下级簇头和簇节点的入侵和响应.由于每一节点都驻有 IDS,过多占用网络资源,由于采用多级结构,该方案易扩展到多层的 MANET.

方案四:Sun B 等提出了基于区域的双层不重叠的入侵检测模式^[6],将网络分成互不重叠的区域,节点分为域内节点和域间节点,域间节点类似于簇头.该方案如同 Sterne D 等提出的方案,由于每一节点都驻有 IDS,过多占用网络资源.

以上方案都采用了类似簇的结构,适用于规模较大的 MANET, Huang Y 仿真表明:在同一的检测率条件下,采用簇结构比不采用簇结构,可以减少 29% 的 CPU 使用率.然而,这几种方法仍有不必要的监控负荷,如重复节点、数量过多的小簇.

3 基于区域的分级 IDS

基于区域的分级 IDS 将网络分成三层,第一层为普通节点,第二层为簇头,第三层为域头.

该方案将网络划分成若干区域,每一区域由一些相邻节点构成,区域内建立若干簇,域间和簇间都无共享节点,以避免对节点的重复监控,减少不必要的资源浪费.

考虑到网络带宽和节点能量、计算资源有限的特点,只在簇头和域头设置 IDS agent.每一簇内设一簇头,簇头内设有 IDS agent,负责簇内数据收集和检测,并上报域头.每一区域设一域头,负责域和簇的形成,并设有 IDS agent,负责域内入侵检测和响应,域头对域内各簇头上报的数据进行聚集并进行相关运算,并与其他域头协作产生全局入侵响应.

3.1 域的形成

域的建立过程如下:首先,由一些具有 1 个或 2 个邻居节点的边界节点启动域建立,边界节点宣称自己为初始节点,并开始建立域.将边界节点作为初始节点,可以避免形成较小的簇.

域内必须要有一个域头,决定是否合并其他域,或接受其他域的合并.刚开始,所有的节点都是单个成员域,即只有其一个节点—初始节点,其作为域头,发送包含其域大小的初始化消息,邻居域头返回其所属域的大小(即节点数的多少),初始节点决定是否合并,标准是合并后域的尺寸不能超过预先设定的门限值.

初始节点将域初始化消息发送给所有的邻居域头,若在同一初始化时间内接受到多个邻居域头返回的初始化响应消息,那么初始节点选取尺寸最小的域合并;同理,邻居域头选取域尺寸最小的初始节点发送响应消息,如图 1 所示.当新域合并后,要选举新的域头,标准是除域内邻居节点外,邻居节点数最多的节点.新域头开始新一轮域合并.当域的尺寸

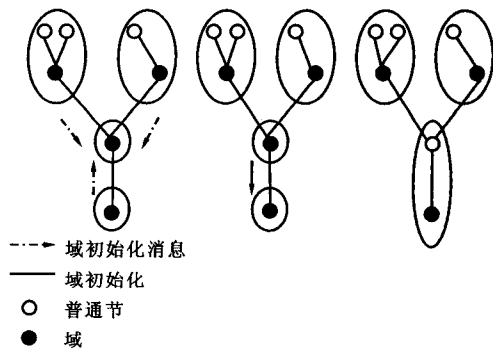


图 1 域的形成

达到域尺寸的最大值时,停止域合并;否则,重复域合并过程.

3.2 簇的形成

域中可以形成若干簇.簇头由邻居节点数最多的节点担任,邻居节点数次多的节点为候选簇头(若邻居节点数相同,则指定簇头),当簇头离开网络或被俘获,候选簇头成为簇头,以避免簇头频繁选举带来更多的资源消耗.一旦簇头选好,其邻居节点被纳入相应的簇.簇之间禁止共享节点.

各域独立运行簇算法,域头为域管理节点,由其发动簇算法.其重复簇选举和簇形成算法,直到簇头所有的邻居节点都纳入该簇或达到簇的最大值.当簇头和候选簇头均离开簇或被俘获,重新运行簇选举算法.

簇选举算法如下:域头发动簇初始化消息给域内所有节点,域内节点响应簇初始化响应消息,该响应消息包括了节点的邻居节点数,域头根据节点的邻居节点数决定簇头和侯选簇头.簇头一旦确定,其与邻居节点形成簇.如图 2 所示.节点 6 的邻居节点数最多,其选为簇头,节点 4 的邻居节点数次多,其选为候选节点;节点 6 和其邻居节点 1,4,5,7 形成第一个簇.重复簇选举过程,直到域内所有的节点都

纳入相应的簇,如节点 2 和节点 3 形成第二个簇,其中节点 2 为簇头,节点 3 为候选节点.

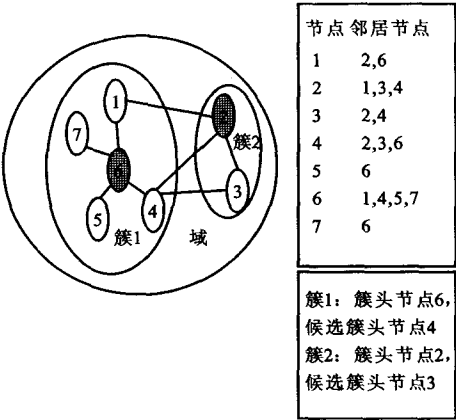


图 2 簇的形成

3.3 仿真

采用 NS-2 作为仿真平台对基于区域的分级 IDS 进行了仿真,并将其与 Huang Y 和 Lee W 提出的方案二从簇的数量、尺寸和孤立簇数量这几个方面进行了比较.仿真实验参数设置为:节点运动范围为 1000m×1 000m 的矩形区域,节点数 n 设为 30、50、100 个,随机移动,移动速率[0m/s,2m/s],模拟时间为 1 000s.仿真结果如表 1 所示.

表 1 簇的比较

	簇的数量			簇的平均尺寸			孤立簇		
	$n = 30$	$n = 50$	$n = 100$	$n = 30$	$n = 50$	$n = 100$	$n = 30$	$n = 50$	$n = 100$
方案二	15	18	32	2.25	3.94	4.5	2	5	14
改进方案	13	15	30	2.22	2.58	3.21	1	3	5

从表 1 可以看出,当网络中节点数 n 为 30、50、100 个时,改进方案的簇数量和孤立簇数量都比方案二的少;与方案二相比,当网络中节点数增加时,改进方案的簇平均尺寸和孤立簇的数量只是缓慢增加,而且节点数越多,改进方案的优势就越明显.

4 结束语

文中提出的一种基于区域的分级 IDS,通过特定的区域和簇形成算法,避免了对节点的重复监控及小簇的形成,减小了不必要的资源浪费;将网络划分成三层,只在簇头和域头设有 IDS agent,节省了资源;簇选举算法使得簇头相对稳定,避免了簇头频繁选举带来的计算与通信负荷.仿真结果表明:与方案二相比,在相同的网络规模下,该方案的簇数量较少、簇平均尺寸增加缓慢,节省了网络资源,而且孤立簇较少,减少了不必要的资源浪费.该方案特别能

适用于分级的 MANET 中.

参考文献:

[1] 李平均,刘权,李天.基于主被动结合的网络入侵检测系统的设计与实现[J].微电子学与计算机,2007,24(7): 50-52.

[2] 解争龙.基于无线 Ad Hoc 网络的入侵检测系统结构研究[J].微电子学与计算机,2007,24(5):103-105.

[3] Kachirski Q, Guha R. Effective intrusion detection using multiple sensors in wireless Ad Hoc networks[C]//Proc. the 36th Annual Hawaii International Conference on System Sciences(HICSS'03). Hawaii,USA,2003:57.

[4] Huang Y, Lee W. A cooperative intrusion detection system for Ad Hoc networks[C]//Proc. the ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'03). Fairfax,VA,USA,2003:135-147.

(下转第 63 页)

模型进行故障诊断的结果都是正确的,它不但可以进行单个故障的诊断,而且还可以完成多个故障源的综合处理。

3 结束语

基于故障树模型和基于神经网络的智能诊断技术是两种不同的诊断技术,将两者相融合可以取长补短。文中采用一种基于故障树模型和基于神经网络诊断技术相结合的新方法用于系统故障诊断,该方法的优点在于:由故障树提取 BAM 神经网络的训练数据,既克服了提取训练数据的盲目性,又可包含系统的全部故障模式。

仿真分析结果表明用这种方法对于系统的故障诊断是有效的,总体方案是可行的。

参考文献:

- [1] 蔡宗平,汤正平,王跃钢,等. 控制系统故障诊断浅析[J]. 电光与控制,2007,14(4):19-22.
- [2] 陈炜,吴志良. 故障诊断专家系统结合故障树技术的结构研究[J]. 航海技术,2005(6):43-44.
- [3] 陈洁,杨兆建,高强. 基于 ANNES 的矿井提升机故障诊

断系统模型[J]. 机械管理开发,2004(2):45-47.

- [4] 郭伟伟. 基于故障树技术的远程故障诊断专家系统的研发[D]. 西安:西北工业大学,2007.
- [5] 王肃宁,杨士元,汪鹏. 基于模式识别进行模拟电路故障诊断的方法[J]. 微电子学与计算机,2004,21(11):113-116.
- [6] 曾水玲,杨静宇,徐蔚鸿. 模糊双向联想记忆网络的有效学习算法[J]. 微电子学与计算机,2007,24(12):70-72.
- [7] Chang Hong, Feng Zuren. Object recognition and tracking with maximum likelihood bidirectional associative memory networks[J]. Neurocomputing, 2008, 72(1/3):278-292.
- [8] Hong Yingyi, Lee Lunhui. Cheng Henghsing. Application of fuzzy fault-tree analysis to assess the reliability of a protection system for a switchyard[J]. International Journal of Emerging Electric Power Systems, 2008,9(4):145-160.

作者简介:

苗伟女,(1982-),硕士研究生.研究方向为故障诊断、智能检测、变频器技术。

范波男,(1975-),博士,硕士生导师.研究方向为无线传感器网络、信息融合、多智能体系统等。

(上接第 59 页)

- [5] Sterne D, Balasubramanyam P, Carman B, et al. A general cooperative intrusion detection architecture for MANETs [C]//Proc. the 3rd IEEE International Workshop on Information Assurance(IWIA'05). University of Maryland, USA, 2005:57-70.
- [6] Sun B, Wu K, Pooch U W. Alert aggregation in mobile Ad Hoc networks [C]//Proc. the 2003 ACM Workshop on

Wireless Security in Conjunction with the 9th Annual International Conference on Mobile Computing and Networking. San Diego, California, USA, 2003:69-78.

作者简介:

程铃女,(1974-),硕士,讲师.研究方向为移动通信网络、计算机网络。