基于Agent的无线传感器网络入侵检测系统

赵建华,刘 宁
(商洛学院 计算机科学系,陕西 商洛 726000)

摘 要:为了提高分簇无线传感器网络的安全性,设计了一个基于Agent的轻量级入侵检测系统。系统由监测Agent,检测Agent,响应Agent和控制Agent等四个Agent组成,它们之间进行相互协作,共同完成检测任务。为了节省能量,簇头节点选取簇内具有高能量、高信誉度的节点作为巡查节点,在预设的时间片段中,巡查节点监测簇内节点通信行为,其他节点处于休眠状态;为了减小误检率,巡查节点检测出信誉度为零的恶意节点后,需要簇头节点对其进行二次诊断。仿真实验表明,系统具有良好的检测率和较低的能耗。

关键词:无线传感器网络;入侵检测;代理;二次诊断
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2011)07-0165-03

An Intrusion Detection System for Wireless Sensor Network Based on Agent

ZHAO Jian-hua,LIU Ning
(School of Computer Science,Shangluo University,Shangluo 726000,China)

Abstract:To improve the security of clustering-based wireless sensor network (WSN),designed a lightweight intrusion detection system (IDS) based on agent. It was made up of four agents -monitor agent, detection agent, response agent and control agent,the four agents worked together to accomplish detection. To reduce energy consumption, cluster head chose one node with highest energy and credibility as monitor node . In the allotted time, the monitor node monitored communication behavior while others were sleep. To reduce false alarm rate,the cluster head carries out second diagnosis mechanisms for malicious after the monitor node found out it. Simulation result showed that the system had good detection rate and low energy consumption.

Key words:wireless sensor network;intrusion detection system;agent;second diagnosis

0 引 言

无线传感器网络(Wireless Sensor Networks,WSN)是由一组计算、存储和能量有限的微型传感器节点通过无线介质构成的自组织分布式网络系统,在环境监测、军事、道路监测等领域有着重要的研究价值[1,2]。传感器网络安全问题尤为突出,缺乏有效的安全机制已经成为传感器网络应用的主要障碍,加之其节点能量、计算、通信和存储能力受限的特点,其安全性问题成为当前研究的热点和难点[3,4]。入侵检测技术作为保障网络安全的一个重要手段,在解决无线传感器网络安全问题上行之有效。因此,根据无线传感器网络的特点,设计一个能耗低、检测率高的轻量级入侵检测系统尤为迫切。

收稿日期:2010-11-30;**修回日期**:2011-03-06
基金项目:陕西省教育科学自然科学研究基金(09JK424);商洛学院教研教改项目(09jyjx03012,09jyjx03015)
作者简介:赵建华(1982-),男,工学硕士,CCF会员,研究方向为无线传感器网络、网络安全。

目前,许多针对无线传感器网络的攻击已经被检测出来,如伪造路由攻击、选择性转发攻击、伪造基站节点攻击、虫洞攻击和泛洪攻击等[5]。Su[6]等人针对分簇式无线传感器网络提出了一种能量节省的入侵检测方案,Ngai等[7]提出了通过检验数据一致性找出一组可疑节点,然后通过分析网络流量信息来判定入侵节点的方法。然而,这些方案要么增加了系统的复杂性和实施难度,对检测的准确率也有一定的影响,要么具有较高的能耗。

文中针对分簇无线传感器网络能量有限的特点,将入侵检测系统分为监测Agent、检测Agent、响应Agent和管理Agent等四个Agent。只有进入工作状态的Agent,才被激活,其他Agent处于休眠状态。为每个节点都安装一个入侵检测系统,但每次只有一个称之为"巡查节点"的节点处于工作状态,完成入侵检测任务,其他普通节点处于休眠状态。巡查节点由簇头选取,具有高能量和高信誉度,每个巡查节点都有工作时间限制,超过限制时间,簇头会重新选取新的巡查节

点。巡查节点检测出信誉度为零的节点时，簇头对恶意节点进行二次诊断。最后，对这种入侵检测机制的检测效率和能耗分别进行实验，并和其他检测系统的性能进行了对比。

1 WSN 模型和 IDS 模型

1.1 分簇 WSN 模型

如图 1 所示，假设的 WSN 基于分簇的结构，所有节点被均匀地部署在监控区域。按照地域的相关性划分成簇，每个簇内有一个簇头和多个普通节点。簇头节点负责簇内节点的管理以及和 Sink 节点的通信，普通节点负责数据信息的采集和相应的检测任务[8~10]。

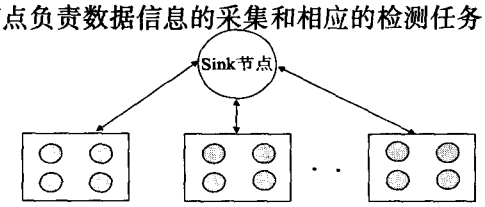

图 1 WSN 模型

1.2 IDS 模型

根据无线传感器网络的特征，每个 WSN 节点都安装一个入侵检测单元（IDU，Intrusion Detection Unit）。每个入侵检测单元由监测 Agent（MA，Monitor Agent），检测 Agent（DA，Detection Agent），响应 Agent（RA，Response Agent）和控制 Agent（CA，Control Agent）等四个 Agent 代理组成。其结构如图 2 所示，以下是四个 Agent 的具体功能。

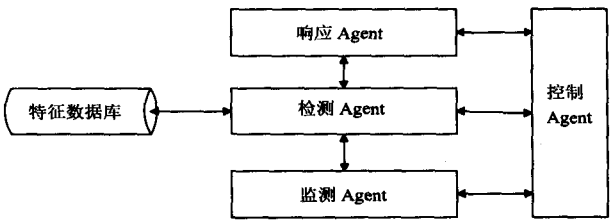

图 2 基于 Agent 的 IDS 模型

（1）监测 Agent。监测 Agent 负责监视收集簇内各个节点的通信信息，并对数据进行采集，将信息经过数据融合、特征提取转化为二进制串，然后发送给各自节点上层的检测 Agent。在该系统中，通信数据采用的数据结构如图 3 所示，由源地址、目的地址、跳数、能量、投递率和流量等字段组成。跳数表示该节点到汇聚节点的距离，投递率是该节点收到的数据包与发送到该节点的数据包数量之比。

2 字节	2 字节	1 字节	1 字节	1 字节	1 字节
源地址	目的地址	跳数	能量	投递率	流量

图 3 数据结构

（2）检测 Agent。当接收到监测 Agent 发送的二进制串信息后，检测 Agent 处于激活状态。检测 Agent 结合特征信息库中内容，对这些二进制串信息进行分析，判断是否有入侵发生，这是整个入侵检测系统最核心的部分。由于检测的数据源大多是基于本地的、不完整的数据信息，检测方法应以异常检测为主，采取的算法在第 2 部分有所介绍。

（3）响应 Agent。当检测模块发现并判断有异常发生时，立即激活本节点的响应 Agent。响应 Agent 主要负责报警信息及相应处理，根据具体的入侵情况采取相应的响应措施，如降低对可疑节点信任度、切断通信、更新通信密钥、重新进行身份认证等。

（4）管理 Agent。管理 Agent 主要负责对监测 Agent、检测 Agent 和响应 Agent 进行管理和维护，并协调它们的工作。同时负责更新特征信息数据库、管理和控制其他 Agent，负责与邻居节点、簇头节点之间的通信，交换检测结果及相关信息。

2 基于节点轮流监测的入侵检测机制

在这种入侵检测机制中，每个节点都有一个初始的信誉度。每次由簇头节点选取一个信誉度高、能量高的节点作为巡查节点，执行入侵检测任务，检测机制如图 4 所示。巡查节点执行入侵检测任务时，簇内其他节点处于休眠状态，直到节点被选取为巡查节点时，才被激活进行入侵检测任务。

具体过程如下：

（1）簇头选取巡查节点进行入侵检测。簇头节点根据簇内各个节点的信誉度、能量等信息选取一个最优节点作为巡查节点完成检测任务，此时巡查节点正式工作。假设节点 m 成为巡查节点，激活节点 m 的监测 Agent，此监测 Agent 监听簇内节点的网络活动信息，如网络流量、能量、跳数等信息，将这些信息进行处理，提呈给 m 节点的检测 Agent，检测 Agent 采用异常检测算法，根据特征库中的信息对这些信息进行检测。如果没有异常，则正常通信；如果判断有异常，比如节点 i 有入侵发生，立即激活本节点（m 节点）的响应 Agent 采取相应的响应措施。

（2）响应 Agent 工作。巡查节点的响应 Agent 根据异常的类型，降低对该异常节点的信任度 Ci（信任度降低的大小与发现异常的情况有关），并将其信誉度降低信息通知给簇内其他邻居节点，然后继续工作。当该入侵节点的信誉度降低为零时，巡查节点判定其为恶意节点。

（3）激活簇头节点。如 i 节点信誉度 $Ci < 0$，则判断该节点为恶意节点，m 节点的响应 Agent 激活簇头节点的响应 Agent，簇头节点对 i 节点进行二次诊断。

（4）簇头节点的二次确诊。为了防止误报或恶意举报，簇头节点要对信誉度小于零的节点进行二次确

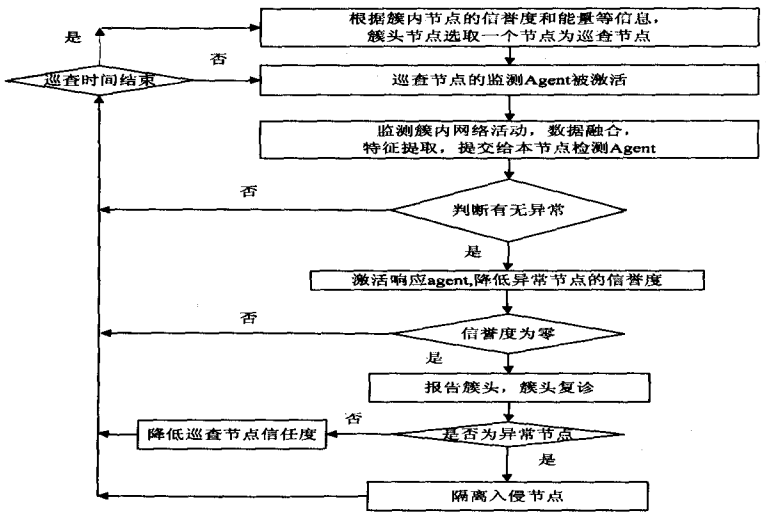

图 4　检测机制

诊,对其身份信息和通信信息再次进行确认,同时为了防止过多的信誉度小于零的节点进行二次确认,采用滑动窗口机制。若确认节点 i 为入侵节点,则切断与该节点 i 的所有通信活动,并广播工作区域内的其他节点,说明节点 i 已经被捕获;若簇头节点判断发现巡查节点 m 对节点 i 的举报有误,则相应降低巡查节点 m 的信誉度 Cm,作为对错误举报的惩罚,这样可以有效降低恶意举报的发生。

(5) 时间片限制。每个巡查节点都有时间片限制,应该在规定的时间内完成监测响应任务,当超过规定的时间,簇头节点重新选取新的节点作为巡查节点。

(6) 数据库更新。当巡查节点工作时间结束时,簇头节点重新选取一个新的节点作为检测节点,并将新的特征数据库复制到新的巡查节点中,同时簇头的特征数据库也进行更新。

其中,采取的异常检测算法如下:

(1)将特征数据库中数据转化为长度为 L 的二进制串。H_n 表示特征库中的数据信息集对应的二进制串集合,H_i 表示集合中的某一个二进制字符串。$H_n = \{H_1, H_2, \cdots, H_n\}$,其中 $H_i = \{h_1, h_2, \cdots, h_L\}$;

(2) 将需要进行检测的数据信息转化为长度为 L 的二进制串 θ,其中 $\theta = \{\theta_1, \theta_2, \cdots, \theta_L\}$;

(3) 计算检测数据信息 θ 与 H_n 中二进制串之间的距离 $D = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{L} | \Theta_j - H_{ij} |$;

(4) 若 $D > \lambda$(λ 为阈值),则表示为异常;否则,将 θ 加入 H_n 中,更新特征库,转(2)。

3　实验仿真

该实验采用 NS2 作为仿真软件,仿真在 100 m × 100 m 的矩形区域中部署了共 50 个节点。MAC 层协议采用的是专门针对低复杂度、低功耗、低数据速率的短距离网络设计的 IEEE 802. 15. 4,网络层采用的是 LEACH 协议,载频是 2. 4 GHz。每个节点的初始能量为 2 J,仿真时间为 1000s。选用的正常流量集为{NS1, NS2},攻击流量集为{AS1,AS2 ,AS3},其中 AS1 模拟 Sinkhole 攻击,AS2 模拟 Hello 洪泛攻击,AS3 模拟 DOS 攻击[11,12]。

节点的平均能耗实验结果如图 5 所示。虚线表示采用节点轮流监测机制的平均能耗,实线表示不采取轮流监测机制的平均能耗。可以看出通过节点轮流检测机制检测入侵,可以大大降低系统的能耗。其中,采用节点轮流监测机制过程中,在 300s 的时候,入侵检测系统检测出异常节点,消耗能量较高;在第 600s 时,巡查节点工作时间结束,和簇头节点进行数据交换,簇头选取新的巡查节点,并完成特征库的更新,这时入侵检测系统的能耗达到最大,之后趋于正常。不过此时的最大能耗也不超过不采用节点轮流检测的系统,进一步说明该系统能耗较低。

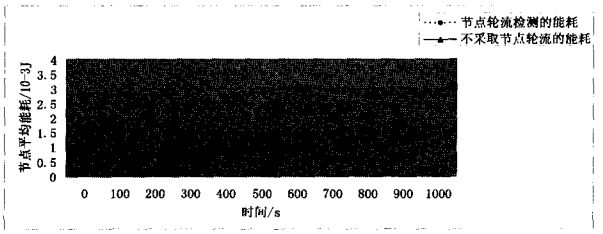

图 5　平均能量消耗

图 6 为误报率和检测率的对比图,从实验结果可以看出,采用二次确认机制后,系统的误报率得到了降低,相应的检测率得到了提高。

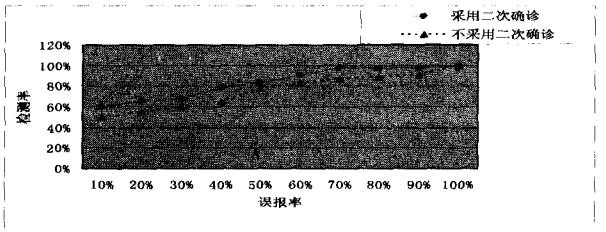

图 6　检测率/误报率

4　结束语

文中针对无线传感器网络能量有限、计算能力有限等特点设计了一个轻量级的入侵检测系统,入侵检测系统中采取多个 Agent 相互配合共同工作。只有处于工作状态的 Agent 才处于激活状态,其他 Agent 处于休眠状态;同时选取具有较高能量和较高信誉的节点,在规定的时间片段内轮流完成入侵检测任务,簇头对信誉度为零的恶意节点进行二次确诊。实验结果表

(下转第 171 页)

全的控制。自动审计部件记录行为的变化,可以实现灾难恢复和叛逆者的追逐,适用于分布式系统。

3)符合面向对象设计的方法,系统易于实现。对于每一个主体或者客体都具备自己的属性,这可以视为该抽象数据类型数据,而改变属性的行为可认为是抽象数据类型的方法。

4)行为有别于使用控制中的责任,基于属性的访问控制中的行为将可能产生灵活的动态效果,首先可以在访问控制的任何时段改变属性信息。第二行为的级联和嵌套符合大型数据库系统及现代访问控制的要求。

4　结束语

作者在研究数字化考试及阅卷系统时,由于考试和阅卷系统的特殊性及试卷信息的敏感性,非常需要一种高效的安全的数字版权管理系统。文中提出的数字版权管理中的基于属性的访问控制模型满足了该系统的要求。该模型比使用控制更符合网上阅卷系统的要求。

文中提出的基于属性的访问控制模型,一方面为数字版权管理中的访问控制提供了一条新的解决方案,另一方面该模型对研究访问控制也具有一定的理论和现实意义。

参考文献:

[1] Zhang Ru, Yang Yu. Digital rights management [M]. Beijing: Beijing University of Post and Telecommunications Press, 2008.

[2] Zou D Q, He L G, Jin H, et al. CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment [J]. Journal of Network and Computer Applications, 2009, 32(2):402-411.

[3] Wang L Y, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control [C] // Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering. New York: ACM, 2004:45-55.

[4] Yuan E, Tong J. Attributed based access control (ABAC) for web services [C] // Proceedings of the IEEE International Conference on Web Services. Washington: IEEE Computer Society, 2005:561-569.

[5] Michael J, Manoj R. A contextual attribute-based access control model [C] // Proceedings of 2006 Workshops on the Move to Meaningful Internet Systems. Berlin: Springer, 2006: 1996-2006.

[6] Yuan E, Tong J. Attributed Based Access Control (ABAC) for Web Services [C] // ICWS'05: IEEE International Conference on Web Services. Orlando: IEEE, 2005:569-575.

[7] 王　立,万世昌,张　珍. 基于互信属性调配机制的访问控制模型[J]. 计算机技术与发展,2009,19(12):127-130.

[8] 张海鑫,程丽红,李顺东. 数字版权管理系统中的使用控制模型[J]. 计算机技术与发展,2009,19(12):135-138.

[9] 李晓峰,冯登国,陈朝武. 基于属性的访问控制模型[J]. 通信学报,2008,29(4):90-98.

[10] 沈海波,洪　帆. 基于属性的授权和访问控制研究[J]. 计算机应用,2007,27(1):114-117.

[11] 田立勤,冀铁果,林　闯,等. 一种基于用户行为信任的动态角色访问控制[J]. 计算机工程与应用,2008,44(19):12-15.

[12] 许　峰,林果园,黄　皓. Web Services 的访问控制研究综述[J]. 计算机科学,2005,32(2):1-4.

(上接第167页)

明,与现有系统进行比较,该系统具有较低的能耗、较低的检测率和较高的误报率。

参考文献:

[1] 裴庆祺,沈玉龙,马建峰. 无线传感器网络安全技术综述[J]. 通信学报,2007,28(8):114-122.

[2] Ian F, Akyildiz, Su Weilian, et al. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4): 393-442.

[3] 孙利民,李建中. 无线传感器网络[M]. 北京:清华大学出版社,2006.

[4] 杨黎斌,慕德俊,蔡晓妍. 无线传感器网络入侵检测研究[J]. 计算机应用研究,2008,25(11): 3205-3209.

[5] 何泾沙,邢　利,张　婷,等. 分簇无线传感器网络的动态入侵检测算法[J]. 北京工业大学学报,2010, 36(6):845-850.

[6] Su W, Chang K, Kuo Y. eHIP: An Energy-Efficient Hybrid Intrusion Prohibition System for Cluster-Based Wireless Sensor Networks[J]. Computer Networks, 2007, 51(4):1151-1168.

[7] 周贤伟,覃伯平. 基于能量优化的无线传感器网络安全路由算法[J]. 电子学报,2007,35(1):54-57.

[8] 李　玲,王新华,车长明. 基于信誉机制的传感器网络安全路由协议设计[J]. 计算机技术与发展,2010,20(9):131-135.

[9] 户晓玲,曾建潮. 基于微粒群模型的移动传感器网络部署研究[J]. 计算机技术与发展,2009,19(10):81-85.

[10] Ngaie E C H, Liu J C, Lyu M R. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks[J]. Computer Communications, 2007, 30 (11-12): 2353-2364.

[11] Meka A, Singh A. Distributed Spatial Clustering in Sensor Networks[J]. Lecture Notes in Computer Science, 2006, 3896: 980-1000.

[12] 武春涛,胡艳军. 无线传感器网络 LEACH 算法的改进[J]. 计算机技术与发展,2009,19(3):80-83.