文章编号：1674-8085(2015)02-0042-06

基于危险理论的无线传感器网络入侵检测的一种新模型

黄 干，*刘 涛

(安徽工程大学计算机应用技术重点实验室，安徽，芜湖 241000)

摘 要：针对传感器节点的内存不足，电池能量有限使得无线传感器网络面临很严峻的安全挑战，提出了一种新式的基于危险理论的无线传感器网络入侵检测系统，它使用了通过 K 最邻近分类器产生的危险信号。实验结果显示这种系统是无线传感器网络的一种新的理想模型。

关键词：无线传感器网络；入侵检测系统；K 最邻近分类器；危险理论

中图分类号：TP393 **文献标识码**：A DOI:10.3969/j.issn.1674-8085.2015.02.011

NEW INTRUSION DETECTION MODEL NOVEL BASED ON DANGER THEORY FOR WIRELESS SENSOR NETWORKS

HUANG Gan, *LIU Tao

（Key Laboratory of Computer Application Technology, Wuhu 241000, Anhui, China）

Abstract: Sensor nodes have insufficient memories and their battery power is limited, so WSNs are facing very serious security challenges and safety issues of WSNs have attracted widespread attentions. We propose a novel intrusion detection system based on danger theory for WSNs that uses a danger signal generated by the K nearest neighbor (KNN) classifier. The experimental results show that this system can effectively reduce our rate of false positive and the energy consumption of the system.

Key words: WSNs; intrusion detection system; KNN classifier; danger theory

0 引言

无线传感器网络是由大量的传感器节点组成的，它们处于开放的环境中，并分散在各个地方。由于无线传感器网络的灵活性、自组织性、容错性、低消耗以及快速部署等特性，使得它已广泛的应用于智能交通、环境监测、工业自动化等领域，得到了工业界和学术界的一致认可[1]。然而无线传感器网络通常部署在无人管理并且环境恶劣的地方或者敌方阵地，加之传感器本身对于攻击是很脆弱的，所以无线传感器网络中传感器节点很容易妥协。与些同时，由于无线传感器网络传递的数据往往都是通过公共的信道进行传递的，所以这些数据很容易被内部或外部的设备所获取。入侵检测是网络抵抗异常和威胁的第二道防线。它有能力监测网络活动，以发现任何恶意行为或入侵行为并尽快地对攻击作出反应，从而减少损失。

典型的免疫系统包括两种防护功能，即先天性免疫和自适应免疫。先天性免疫是由基因决定的，

收稿日期：2014-10-17；修改日期：2014-11-03
基金项目：国家自然科学基金项目(61300170) ；安徽省教育厅重点资助项目(KJ2013A040) ；安徽省自然科学基金项目(1308085MF88)；安徽工程大学青年基金项目(2013YQ28)
作者简介：黄 干(1990-)，男，安徽滁州人，硕士生，主要从事网络与信息安全研究(E-mail:15695538386@163.com);
*刘 涛(1973-)，女，安徽六安人，副教授，硕士生导师，主要从事网络与信息安全研究((E-mail:76627110@qq.com).

从父母那继承而来。而自适应免疫是在系统的先天性免疫不能摧毁一些病原体时形成的[2]。基于生物免疫系统，人类已经开发了很多算法来模拟它，并用这些算法解决了很多领域的复杂问题。现在普遍使用的技术有克隆选择、免疫网络理论、危险理论算法等。前两种技术仅是模拟自适应免疫系统，而危险理论算法主要模拟先天性免疫系统和自适应免疫系统的同时使用。

之前，Kuang 等在文献[3]中提出了一种使用 CSI-KNN 算法的入侵检测模型，他使用两个参数，一个是陌生度，一个是隔离度。陌生度是衡量未知行为是否与正常或异常的行为相似，隔离度是辨别未知行为与正常行为的相似度程度从而侦测异常攻击，最后再集成这两个参数作最后的决定，此外，它还提供一个信任等级。李佳在文献[4]中提出一种基于 KNN 和改进人工鱼群算法选择特征的网络入侵检测模型。它计算特征之间的关联度，采用 KNN 算法消除原始网络数据中的冗余特征，将得到的特征子集作为改进的人工鱼群算法的初始解，通过模拟鱼群的觅食、聚群及追尾行为找到最优特征子集，建立网络入侵检测分类器。冯莹莹等在文献[5]中提出了基于 KNN 和粒子群优化（PSO）选择特征的网络入侵检测模型。它首先采用 K 近邻算法消除原始网络数据中的冗余特征，并将其作为粒子群算法的初始解，然后通过粒子之间信息共享、协作找到最优特征子集来检测入侵。在本文，为无线传感器网络提出一种新的基于危险理论的入侵检测模型，该模型与之前的使用了 KNN 的入侵检测模型的不同之处在于，它通过 K 最邻近分类器产生危险信号并把危险理论与 KNN 很好地融合了起来，异常检测率大大提高，并且耗能不高，更适合无线传感器网络。

本文的其余部分组织如下：第 1 部分简单介绍人工免疫系统和危险理论的相关工作；第 2 部分详细介绍这种新式入侵检测模型的结构及工作原理；第 3 部分给出实验结果并得出结论；第 4 部分对未来工作进行展望。

1 相关工作

1.1 入侵检测国内外研究现状

恶意节点的攻击通常分为内部攻击和外部攻击。大部分的外部攻击都可以利用防火墙技术很好地拦截。相比于外部攻击，在网络上的内部攻击危险更让人们更感到棘手，而入侵检测是一种处理内部攻击的很好的方法。

最近，研究者在入侵检测领域有了很多研究成果[6-9]。在文献[6]中，Wang 等提出一种基于信任的入侵检测。在该入侵检测模型中，它使用数据包标记和启发式排名算法来辨别网络中可能的恶意节点。每个数据包会被加密和填充从而隐藏发送数据包的来源。数据包被标记是为了方便恢复数据的来源，并计算每个节点的丢包率。在文献[7]中，Ting SUN 等提出一个基于代理的入侵检测模型。该模型采用分布式的结构去监测入侵行为，并在本地节点实现异常事件的处理。该模型可以使得妥协节点自动恢复并有效抵御 DoS 攻击对网络的破坏。在文献[8]中，H Sedjelmaci 等提出一个基于节点行为的入侵检测模型。在该模型中，入侵检测是在簇头节点和簇内成员节点上完成的，这很好地缓解了网络上的安全威胁，并且网络中的代理也相互协作来探测恶意节点，这也提高了侦测入侵的准确性。在文献[9]中，傅蓉蓉等提出一种基于危险理论的无线传感器网络入侵检测模型。该模型引入分布式节点合作机制，不需要在每个节点上运行一个完整的检测实例，并且该模型只有感知到危险后才进行异常识别，这些都大大减少了整个网络的检测开销。

1.2 危险理论

危险理论强调外来抗原可以通过危险信号来检测。不管恶意抗原什么时候入侵细胞，都可以引起危险信号。Matzinger 在文献[10]中提出，危险信号是由受难细胞引起。所以，辨别细胞死亡是正常死亡还是非正常死亡是检测人体外来抗原的一个关键。从原理上说，细胞正常死亡是指一个细胞自然条件下死亡，细胞非正常死亡是指一个细胞受到外来抗原，受伤从而引起的一个意想不到的死亡[11]。这个辨别过程主要是运用三信号规则框架[12]。根据这一框架，第一个信号是初始化信号（IS），它是由非正常死亡的细胞引起的初始化检测过程；第二个信号是识别信号（RS），用于抗原检测；第三个信号是协同刺激信号，用来确保细胞死亡是由抗原引起的。这些信号的相关性确保 T 细胞正常地识别细

胞死亡是正常的还是非正常的。一旦检测外来抗原，这个死亡细胞就会在它周围产生一个空间区域，称为危险域，并在此区域内减轻并局部化攻击的影响[13]。

受危险理论的启示，把危险理论应用到计算机网络的异常检测中。在本文所提出的入侵检测模型中，并不会检测每一个外来的细胞。只有当细胞非正常死亡并发出危险信号时，危险才会被检测到。通过危险理论，可以仅仅处理危险信号而并不是任何非自体信号。这样大大减少了系统的误报率，提高了检测的速度和效率。

1.3 KNN 算法

KNN 是一个有监督的无参数分类算法[14,15]。该算法需要先找到待分配标签节点的 K 个最邻近已分配标签的节点，然后进行投票，找出占多数的标签内容，把它分配给待分配标签的节点作为标签内容。为了找出最近的邻居，计算距离很关键的。

大部分 KNN 分类器使用欧几里德距离公式来计算代表输入向量的相似性，计算公式如下：

$$d(x_i,x_j)=\sqrt{\sum_{r=1}^{n} w_r(a_r(x_i)-a_r(x_j))^2} \qquad (1)$$

定义向量 $x=(a_1,a_2,...,a_n)$ 作为例子， n 向量维数，也是属性个数。a_r 例子的第 r 个属性，w_r 是第 r 个属性权值。$d(x_i,x_j)$ 越小，两个例子越相似。

分类标签由 K 个最邻近邻居占多数的标签决定的，公式如下：

$$y(d_i)=\arg\max_K \sum_{x_j\in KNN} y(x_j,c_k) \qquad (2)$$

d_i 是测试用例，x_j 是它的 K 个最邻近的邻居之一，$y(x_j,c_k)$ 表示是否属于类 c_k。公式（2）表明测试用例所属的类是 K 个最邻近的邻居所属的类。

本文中将结合人工免疫网络和 K 最邻近分类器在危险理论领域为无线传感器网络提出一种新颖的入侵检测模型。

2 所提出的模型

在无线传感器网络中，入侵检测是安全应用中一个很重要的研究课题，可以使用自适应免疫系统和先天性免疫系统来提高它。为了实现这个目的，使用人工免疫网络作为自适应免疫系统，在先天性免疫系统使用 KNN 分类器来产生危险信号。表 1 给出了危险理论 AIS 到系统模型的隐喻。

提出的模型方法如下：

（1）自适应免疫系统通过 APC 给每个抗原分配一个初始标签。

（2）通过 KNN 分类器来分析抗原的邻居。如果抗原的周围环境是危险的，便会产生危险信号。

（3）决者者模块收到自适应免疫系统的初始标签和先天性免疫系统的危险信号以后，如果只有危险信号，而初始标签为“正常”，则认为输入抗原为未被识别器所辨别的未知非已，它会为输入抗原分配“不正常”为最终标签；如果初始标签是“不正常”并且它又从先天性免疫系统收到一个危险信号，则它就会为输入抗原分配“不正常”标签；如果初始标签是“不正常”，但是却没有从先天性免疫系统那收到危险信号，则认为该抗原原本为“正常”，是被误识别为“不正常”，它从而为输入抗原分配“正常”作为最终标签；如果初始信号是“正常”并且没有收到危险信号，则为输入抗原分配“正常”为最终标签。

表 1 危险理论 AIS 到系统模型的隐喻

Table 1 Metaphor from AIS to the system model in the danger theory

AIS	IDS 模型
病原体	入侵节点或具有传播性的蠕虫和病毒
抗原	用于识别攻击的信号参数信息
受难细胞	由于受到入侵影响，感知到危险的节点
APC 细胞	自适应免疫系统模块探测器
DC 细胞	先天性免疫系统模块
淋巴细胞	决策者模块
B 细胞和 T 细胞	免疫应答节点
抗体	决策者模块发出的对策信息

2.1 自适应免疫系统模块

人工免疫网络是人工免疫系统中使用比较广泛的方法之一。在本论文中，使用这个模型来执行自适应免疫系统模块中的算法。该模型的学习过程如下:

（1）先随机生成一些抗体，把它作为最初的网络节点。

（2）为了让网络学习，把训练集中的抗原提呈

给网络。对于抗原，需要计算与网络中所有节点之间的亲和力。

（3）根据抗体与抗原之间的亲和力，选中一些亲和力较高的抗体：亲和力越高，克隆数目越多[16]。而对于亲和力较低的抗体，按亲和力进行变异：亲和力越低，变异可能性越高。最后选择亲和力高的抗体成为记忆抗体，加入到原来的网络中。

（4）在新的网络中删除太相近的数据。如果记忆抗体与原来的抗体之间的亲和力小于一定的阈值就被消除；与抗原的亲和力小于一定阈值的抗体也被消除；最后再随机加入一些新的抗体到网络中。

探究机制在免疫系统是一个强有力的免疫力量，它学习如何对一个之前从未见过的抗原进行免疫应答。所以，可以使用人工免疫网络去给抗原一个初始标签。使用该方法之间需要定义一些参数。当使用人工免疫网络给抗原分配初始标签以后，把抗原提呈给决策者模块。

1- 初始化 B 细胞和抗原
2- 为每个抗原重复下列步骤：
  1. 自适应免疫系统
    i. 提呈抗原给检测器；
    ii. 分配初始标签给抗原；
  2. 先天性免疫系统
    i. 评估抗原的环境；
    ii. 使用危险信号来报告危险环境；
3- 决策者模块通过自适应免疫系统和先天性免疫系统来为抗原分配最终标签

图 1 提出模型的描述

Fig.1 Description of the model proposed

2.2 先天性免疫系统模块

在人体内，先天性免疫系统的关键任务就是产生危险信号。在本文，使用 K 最邻近分类器（K nearest neighbor classifier）来完成这个关键任务[17]。这个分类器为了去评估每个抗原节点，从抗原训练集中找出 K 个最邻近节点。然后 K 个最邻近节点进行投票，如果大多数邻居有正常标签，则认为评估的节点所处的环境是安全的；否则被评估节点就产生危险信号，并以被评估节点为中心产生危险区域。如前面所提到的，在模型中，先天性免疫系统为危险环境产生一个危险信号，并把这个信号送给决策者模块。

2.3 决策者模块

决策者模块负责为输入抗原分配最终标签，并触发免疫应答。

决策者在收到自适应免疫系统模块发来的初始标签和先天性免疫系统模块发来的危险信号来确认是否发生了入侵[18]。一旦发现入侵，淋巴细胞产生与提呈细胞发生的抗原相匹配的抗体，消灭病原体。也可以激活 T 细胞，产生毒性 T 细胞来杀死病原体。

3 实验与结果分析

3.1 参数配置

本文使用 Matlab 来仿真 WSNs，仿真出来的 WSNs 如图 2 所示。为了评估提出的入侵检测模型的检测结果，需要一组有着正常和不正常标签的数据集，首先产生 27172 个正常类型的数据集和 24917 个不正常类型的数据集。然后实验使用了在正常和攻击状态下通过监控一个远程过程调用（RPC）而产生的数据集 rpc.statd 来验证模型。

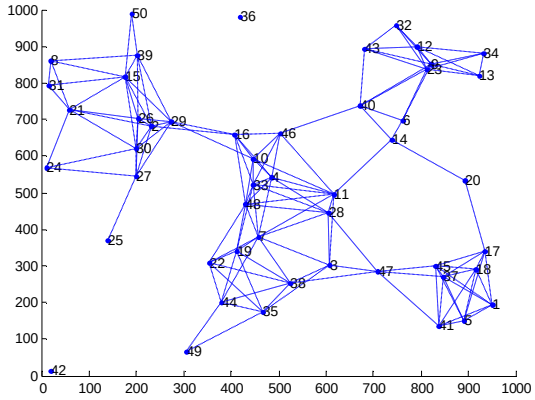

图 2 WSNs 的仿真情景

Fig.2 Simulation scenario of WSNs

这个实验在 Matlab 平台下进行，提出模型的性能是由运行结果的平均水平来评估的。参数如表 2 所示。在评估前，正常化每个类型，从数据集中删除冗余类型的数据来增加实验速度。

3.2 结果分析

有很多参数用来检测 IDS，而在这里，把提出的模型与基于免疫网络的模型从二个主要参数进行对比：检测率和误报率。

检测率定义为节点成功检测出全部恶意节点的比率。这个度量暗示着模型的效率，它的范围从 0 到 1 。结果如图 3 所示。

如图 3 所示，两种模型的检测率都处于上升阶段。然而，从 400 秒以后，提出的模型的检测率明显高于基于免疫网络的模型。这个现象的原因主要归结为 KNN 最邻近分类器对检测恶意节点方面的显著性和有效性。

表 2　参数设置

Table 2　Parameter settings

参数	值
节点个数	50
网络大小（m）	1000×1000
最大范围半径（m）	200
数据包大小（Byte）	56
包转发率（kbps）	19.2

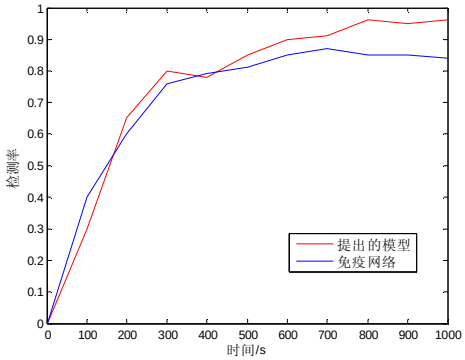

图 3　检测率与时间的关系对比图

Fig.3　Relation comparison chart between the detection rate and the time

误报率定义为误判节点类型的比率。它的范围从 0 到 1。误判节点可以分为两种：一种是把正常节点判断为恶意节点，另一种是把恶意节点判断为了正常节点。实验结果如图 4 所示。

如图 4 所示，很容易看出提出模型的误报率低于基于免疫网络的入侵检测模型。提出的模型是通过多个邻居投票决定，因此可提高判断的准确性。此外，最后的判断是通过把危险信号和初始标签一起结合来判断的，减少了误判。从这两点看，提出的模型能维持一个比较低的误报率。

从图 5 可以看出，提出的模型随着时间的增长，检测率总在 85%~94%之间。它表明系统的能耗并不是太大，而整个系统的能量消耗不会随着时间的推移而增加。

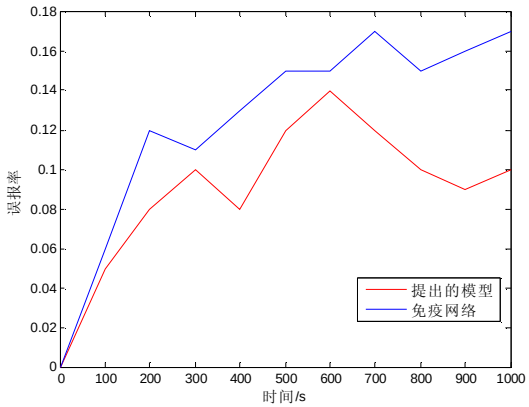

图 4　误报率与时间的关系

Fig.4　Relationship between the false positive and the time

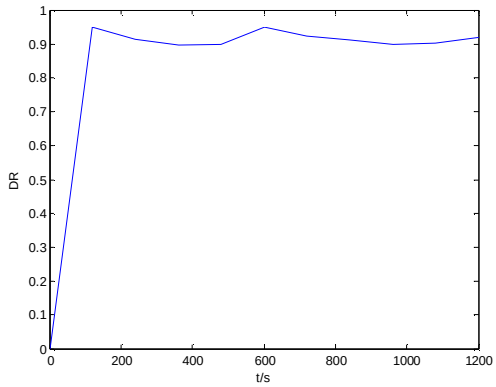

图 5　提出的模型检测率与时间的关系图

Fig.5　Diagram between the detection rate and the time in the proposed model

4　结束语

本文提出一种新的基于危险理论的入侵检测模型，在不消耗太多能耗的情况下，减少了误报数量。通过仿真工具 Matlab 对该入侵检测模型进行了建模，模拟不同场景下 WSNs 攻击节点的流量，并与传统的基于免疫网络的入侵检测模型进行了比较，它有着更高的检测准确率和更低的误报率，并且对系统能耗不是太大，从而延长了无线传感器网络的工作时间。在未来的研究中，该系统还需要进一步的研究，比如，危险信号的定义和获得危险信号的过程还需要继续研究。

参考文献：

[1] Gungor V C, Lu B, Hancke G P. Opportunities and challenges of wireless sensor networks in smart grid[J]. IEEE Transactions on Industrial Electronics, 2010, 57(10): 3557-3564.

[2] Arnold J N, Wormald M R, Sim R B, et al. The impact of glycosylation on the biological functionand structure of human immunoglobulins[J]. Annu. Rev. Immunol., 2007, 25: 21-50.

[3] Kuang L, Zulkernine M. An anomaly intrusion detection method using the csi-knn algorithm[C]. Proceedings of the 2008 ACM symposium on Applied computing. ACM, 2008: 921-926.

[4] 李佳. 基于 AFSA-KNN 选择特征的网络入侵检测[J]. 计算机工程与设计, 2014, 35(8): 2675-2679.

[5] 冯莹莹, 余世干, 刘辉. KNN-IPSO 选择特征的网络入侵检测[J].

[6] Wang C, Feng T, Kim J, et al. Catching packet droppers and modifiers in wireless sensor networks[C]. The 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, 2009:1-9.

[7] Sun T, Liu X. Agent-based intrusion detection and self-recovery system for wireless sensor networks[C]. The 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT). IEEE, 2013: 206-210.

[8] Sedjelmaci H, Senouci S M. Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks[C]. Global Information Infrastructure Symposium, 2013. IEEE, 2013: 1-6.

[9] 傅蓉蓉, 郑康锋, 芦天亮, 等. 基于危险理论的无线传感器网络入侵检测模型[J]. 通信学报，2012, 33(9): 31-37.

[10] Matzinger P. Tolerance, danger, and the extended family[J]. Annual review of immunology, 1994, 12(1): 991-1045.

[11] Mohsin M F M, Bakar A A, Hamdan A R. Outbreak detection model based on danger theory[J]. Applied Soft Computing, 2014, 24: 612-622.

[12] Lo N W, Yohan A. Danger theory-based privacy protection model for Social Networks[C]. 2014 Federated Conference on Computer Science and Information Systems (FedCSIS).IEEE, 2014: 1397-1406.

[13] Wang W, Zhang C, Zhang Q. An Anomaly Detection Model Based on Cloud Model and Danger Theory[M]. Trustworthy Computing and Services. Springer Berlin Heidelberg, 2014: 115-122.

[14] Zhang C, Li F, Jestes J. Efficient parallel kNN joins for large data in MapReduce[C]. Proceedings of the 15th International Conference on Extending Database Technology. ACM, 2012: 38-49.

[15] Steenwijk M D, Pouwels P J W, Daams M, et al. Accurate white matter lesion segmentation by k nearest neighbor classification with tissue type priors (kNN-TTPs)[J]. NeuroImage: Clinical, 2013, 3: 462-469.

[16] Xian-jin F, Miao-qi C A I. 基于人工免疫系统的入侵检测研究[J]. 计算机工程, 2013, 39(11): 136-138,142.

[17] Hedayat M R, Moghadam A M E. An Adaptive Artificial Immune Network Classifier with Independent Suppression Threshold[C]. 2011 International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC). IEEE, 2: 138-142.

[18] 田志宏, 王佰玲, 张伟哲, 等. 基于上下文验证的网络入侵检测模型[J]. 计算机研究与发展，2013, 50(3): 498-508.