基于危险理论的无线传感器网络入侵检测模型

傅蓉蓉[1]，郑康锋[2]，芦天亮[2]，杨义先[1,2]
(1. 北京交通大学 计算机与信息技术学院，北京 100044；2. 北京邮电大学 信息安全中心，北京 100876)

摘 要：针对无线传感器网络入侵检测技术面临的挑战，利用了人工免疫技术的基本原理，提出一种基于危险理论的入侵检测模型。模型采用了分布式合作机制，与采用混杂模式监听获取全局知识的方法相比，在检测性能和能耗上都具有优势。仿真结果表明，相比于传统的单一阈值 Watchdog 算法和自我-非我(SNS)模型，基于危险理论的检测模型能够提供较高的检测率和较低的误检率，并且有效降低了系统的能耗。

关键词：无线传感器网络；入侵检测；人工免疫系统；危险理论
中图分类号：TP393 **文献标识码：**A **文章编号：**1000-436X(2012)09-0031-07

Danger theory inspired intrusion detection model for wireless sensor networks

FU Rong-rong[1], ZHENG Kang-feng[2], LU Tian-liang[2], YANG Yi-xian[1,2]
(1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2. Information Security Centre, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: According to the challenges of intrusion detection technique for wireless sensor networks, a danger theory inspired intrusion detection model was proposed by taking advantage of the working principle of artificial immune system. Due to the distributed and cooperative mechanism, the proposed model shows more advantages in detection performance and energy consumption than methods adopt promiscuous to get global knowledge. The simulation results show that compared to traditional Watchdog algorithm with single threshold and self-nonself (SNS) model , the model inspired by danger theory can provide highest correct detection rate and lowest false detection rate. Moreover, the model can also decrease the energy consumption of the system.

Key words: wireless sensor networks; intrusion detection; artificial immune system; danger theory

1 引言

由于传感器网络的缺乏人工干预及资源受限的特点，使得无线传感器网络的入侵检测面临着巨大的挑战。近年来生物免疫启发的人工免疫系统（AIS）由于其在工作原理上与入侵检测的一致性得到了广泛的关注，AIS 的基本特征包括：自组织、分布式、高顽健性、轻量级、多层次及多样性等。这些特征使其在入侵检测方面体现出了优势并取得了一定成果[1,2]。

早期的研究中，自我-非我 (SNS, self-nonself) 模型在 AIS 领域得到了深入的研究，这种模型将抗原空间分为 2 种，一种是自我抗原，另一种是非我抗原。自我抗原被用作为淋巴细胞（如 B 细胞）的训练基础数据，那些会引起自身免疫反应的淋巴细胞将被删除，即免疫耐受，而通过了免疫耐受的淋

收稿日期：2011-12-23；**修回日期：**2012-05-19
基金项目：国家科技重大专项基金资助项目（2011ZX03002-005-01**）；国家自然科学基金资助项目（**61070204, 61101108**）**
Foundation Items: National S&T Major Project (2011ZX03002-005-01); The National Natural Science Foundation of China (61070204, 61101108)

巴细胞将存活下来，称为成熟的淋巴细胞，它们用来攻击外来抗原以便保护机体的安全；而非我抗原却是构成机体威胁的物质，也就是淋巴细胞的应答对象。SNS 免疫模型的思想是免疫应答由抗体表面受体对外来抗原的识别而诱导的，即由非我抗原触发免疫应答，非我抗原通过激活抗原提呈细胞（APC, antigen presenting cell）提呈的抗原并产生响应。

但是免疫系统对于人们吃的食物中的外界细菌或者对一些明显发生细胞突变的肿瘤等异己抗原不发生免疫响应，所以自我-非我模型的合理性受到了质疑。1994 年，Matzinger [3]首先提出危险理论，认为免疫系统所能区分的实际上是“从某些非我中区分出某些自我”。危险理论假定免疫系统的激活不是由非我的检测唯一决定，也不对一个潜在的入侵做出响应，直到危险被检测到。

受到生物领域中危险理论的启发，本文提出了基于危险理论的无线传感器网络入侵检测模型。并通过仿真实验验证了提出的模型在检测率、误检率和能量消耗方面具有优势。

2 相关工作

2.1 危险理论

危险模型在细胞和信号的基础上增加了额外的一层，认为 APC 由受难细胞（如受到病原体侵入、毒素侵入、创伤等影响的细胞）发出的危险信号触发，而不一定是非我触发的，危险信号被 APC 识别，是引起免疫应答的关键因素。图 1 描述了危险模型中免疫应答的响应。免疫过程可分为以下步骤：一个非正常死亡的细胞发出了一个危险信号；邻近的抗原提呈细胞 APC 被激活并开始识别和捕获抗原；APC 通知本地的淋巴结并把所识别的抗原提呈给淋巴细胞；淋巴细胞产生抗体进行抗原识别。

从本质上讲，危险信号的产生将会在受难细胞周围建立一个危险区域，在危险区域内的淋巴细胞才会被激活，产生大量的对应能匹配该抗原的抗体。而那些不在危险区域内的淋巴细胞则不被激活，因而也不能产生抗体。

虽然危险理论在传统的生物免疫领域仍然存在争议，但是危险理论相比 SNS 模型更加适用于入侵检测领域[4,5]。危险模式应用于无线传感网络的入侵检测主要存在以下 2 个优点：1) 发生危险时才会触发检测过程，可以降低误检率并且降低不必要的能量消耗；2) 危险域可以根据不同的危险程度或者安全策略来确定，可以提高检测系统的灵活性。

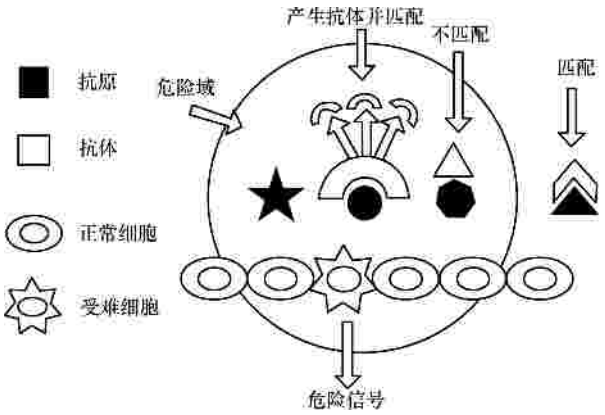


图 1 危险模型中免疫应答的响应

2.2 人工免疫启发的入侵检测

当前，将危险理论应用于入侵检测的工作主要集中在主机或者互联网领域，而关于无线传感网络的研究则不多。Junwon Kim 等人[6]通过危险理论相关算法解决了针对 DD 路由协议的 Interest Cache Poisoning 攻击，文章仅利用了节点本地的缓冲区信息，并没有考虑如何获取全局知识。

Martin Drozda 等人[7~9]将 AIS 引入传感网络，解决丢弃、延迟转发数据分组和 Wormhole 等问题。文章采用了 SNS 检测模型，同时为了获得全局的信息，引入了 Watchdog 算法[10]。提出让节点处于在混杂模式下，监听通信范围内的数据流量，并将监听到的信息编码成基因进行模式匹配。文献[11,12]将 AIS 的工作原理用于传感网络的入侵和响应，但是同样采用了混杂模式获得两跳邻居节点的通信信息。混杂模式虽然能够提供全局知识，但是这种模式阻止了节点进入睡眠，强制其进入空闲或接收状态，极其消耗能量。研究表明，传感器节点的大部分能量消耗在无线通信模块，传输 lbit 信息所消耗的能量大约是执行一条计算指令所消耗能量的 3 000 倍[13]。

此外，大多数的研究[6~9]将单个节点模拟成一个人体，程序或者其他的计算单元模拟组织、器官或者细胞。这就导致需要在单个节点上运行整个检测实例，这在资源受限的传感网络中是不实用的。

本文的目的是设计一个分布式和分层的检测模型，在无线传感网络中为危险理论建立一个合理隐喻。利用危险理论的优势，终端节点只需检测自

身本地的信息感知危险，并合作提供全局知识。

2.3　IEEE 802.15.4

IEEE 802.15.4 标准提供了对无线传感器网络物理层及媒体接入层的具体描述，而这 2 层的信息都可以由节点从本地获得。通过节点监视本地的信息发现危险可以避免节点处于混杂模式以节省能量。同时 IEEE 802.15.4 提供了一个天然分层的结构，这种结构在信息管理和聚合方面表现出了强大的优势。

IEEE 802.15.4 使用了 CSMA/CA 协议[14]接入物理媒介，这个协议提供了冲突避退机制，在节点开始传输数据之前，需要首先侦听信道并持续一个预定义的时间，如果信道忙碌，节点需要等待一个特定的时间再重新尝试。同时 IEEE 802.15.4 支持 ACK 确认机制保证数据的可靠传输。

2 种节点存在于 IEEE 802.15.4，FFD 和 RFD。FFD 可以作为 PAN 协调器、路由和终端，但是 RFD 只能作为终端。这种节点类型的划分可以提供分层的网络拓扑，在这种分层网络中被入侵节点影响的节点只需将自身的信息传输给中心 PAN 协调器，PAN 协调器便能获得全局信息来做出入侵判决。

3　系统模型

根据危险理论，受难细胞发出危险信号，并在其周围建立一个危险区域，其中的抗原被 APC 捕获，APC 提呈抗原提供共同刺激信号，从而引起了免疫应答。在免疫应答过程中，淋巴细胞产生与危险域内的抗原匹配的抗体。

本文利用危险理论的工作原理，将检测过程分成 3 个阶段：危险感知阶段、抗原提呈阶段和决策阶段，图 2 描述了本文提出的检测系统模型。

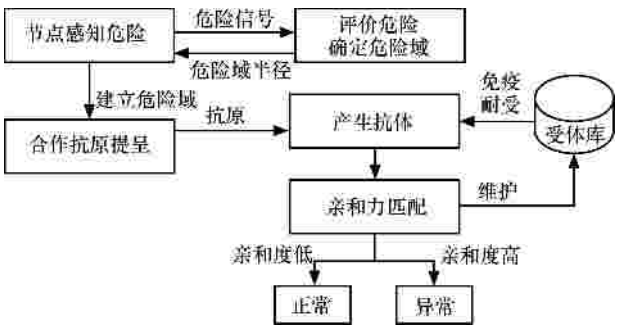


图 2　入侵检测模型

从能源的角度来看，每个节点同时运行一个完整的检测实例是不合适的。所以本文利用 IEEE 802.15.4 的分层结构实现合作式检测，边界终端节点只需检测自身属性的变化来感知风险，中心节点（称作决策节点）收到危险后确定危险程度及危险域的大小并要求获得抗原，危险域内的节点合作提供网络流量信息形成抗原，中心节点负责产生抗体，动态地维护抗体，并将抗体与抗原进行匹配确定是否发生了入侵。表 1 给出了基于危险理论的 AIS 到本文系统模型的隐喻。

表 1　危险理论 AIS 到系统模型的隐喻

危险理论 AIS	系统模型
淋巴细胞	检测节点和决策节点
病原体	入侵节点或者具有传播性的蠕虫、病毒
凋亡细胞	由于能量耗尽等原因正常不工作的节点
受难细胞	由于受到入侵影响，感知到危险的节点
危险信号	发送给决策节点表明存在潜在入侵的信息
APC	危险域中的节点合作提供抗原
抗原(antigen)	危险域中的全局信息
抗体(antibody)	由耐受过程产生的异常模式
受体(receptor)	抗原和抗体都由受体构成，每个受体描述每个节点流量信息的正常模式

3.1　危险感知

在生物免疫系统当中，如果一个细胞由于正常原因死亡（凋亡细胞），细胞实体在分解之前就会被清除掉。但是由于非正常原因坏死的细胞（受难细胞）会分解实体并且释放出危险信号。类似地，在本文提出的模型中，节点感知自身的变化发现危险并释放出危险信号，通常情况下，节点能够在失去工作能力之前发现危险并且做出反应。

节点自身属性的异常变化反应了潜在的危险。节点的物理层和媒体接入层的属性都可以本地获得，所以本文关注这 2 层的属性信息。用来感知危险的属性用 DFi(danger features)来表示。

DF1　电源能量下降速率。传感节点是资源受限的，对 DoS 类攻击非常敏感。*DF*1 的计算式为

$$DF1=C_{\text{power}}/?\,t \tag{1}$$

其中，C_{power} 表示在$?\,t$ 时间内电能的变化量。

DF2　数据分组发送回退频率。由于采用了冲突避退机制，当发生分组阻塞攻击时，这个属性的变化明显。*DF*2 的计算式为

$$DF2=\sum_{t}^{t+\Delta t} N_{\mathrm{BP}} \Big/ \Delta t \tag{2}$$

其中，$\sum_{t}^{t+\Delta t} N_{\mathrm{BP}}$ 表示在$?\,t$时间内回退的数据分组个数。

DF3　平均回退持续时间。此属性的变化可以发现持续的阻塞干扰类攻击。*DF*3 的计算式为

$$DF3=T_{\mathrm{BP}}/?\,t \tag{3}$$

其中，T_{BP} 表示在$?\,t$时间内总共回退等待的时间。

DF4　ACK 成功率。在发送数据之后，节点通常希望获得 ACK 以证实数据发送成功，ACK 成功率过低也表明存在危险。*DF*4 的计算式为

$$DF4=\sum_{t}^{t+\Delta t}(N_{\mathrm{ACK}} / N_{\mathrm{SP}}) \tag{4}$$

式(4)计算了在$?\,t$ 时间内发送的数据分组的个数与实际收到的 ACK 的个数的比值。

DF5　数据帧接收频率。接收到的数据帧频率的异常变化暗示着危险， 比如节点作为攻击目标时，接收到的数据帧数目增大，接收频率增大。*DF*5 的计算式为

$$DF5 = \sum_{t}^{t+\Delta t} N_{\mathrm{RF}} \Big/ \Delta t \tag{5}$$

DF6　数据帧发送频率。发送的数据帧数频率的异常变化也暗示着危险，比如发生大规模的蠕虫或阻塞攻击时，节点通常要转发这些恶意的数据分组导致发送数据帧数目增大，发送频率增大。而发生 Sinkhole 攻击时，本来作为正常路由的节点将不再转发数据导致发送数据帧数目骤减，发送频率骤减，计算式为

$$DF6 = \sum_{t}^{t+\Delta t} N_{\mathrm{SF}} \Big/ \Delta t \tag{6}$$

将每个属性归一化，并给定统一的变化阈值 d，在 t 时刻，如果 $CFi=|DFi_t- DFi_{t-1}|>d$，则认为属性 *DFi* 发生了不正常的变化，可能存在危险。

感知到危险之后，节点发送危险信号给决策节点,危险信号表示为

$$DS=<Timestamp, \{(DFi, CFi)\}> \tag{7}$$

危险感知过程可以利用每次节点的正常工作时间，不需要产生额外的调度将节点唤醒。

3.2　抗原提呈

一旦决策节点收到危险信号，便要建立一个危险域，危险域以发出危险信号的节点为中心，覆盖范围称作危险域半径，以跳数为单位。危险域半径与危险程度有关，危险程度表示为

$$D_{\mathrm{danger}}=\sum_{j=0}^{nd}\sum wi_j \cdot CFi_j \tag{8}$$

其中，nd 为一个时间段内，决策节点收到的危险信号的个数。$?\,i$ 为每一个危险属性变化的权重。危险域半径为

$$Ra=\lceil s\times D_{\mathrm{danger}} \rceil \tag{9}$$

参数 s 为保护的无线网络的安全等级，从 *Ra* 的表达式可以看出，危险半径与网络的危险程度和网络的安全等级成正比。

感知到危险的节点在自己 *Ra* 跳范围之内建立危险域，此节点向危险域内的节点广播流量日志获取请求。在一些情况下，比如蠕虫攻击，很多节点感知到危险，危险域就会存在重叠，这种情况下，节点选择最近的节点上传自己的流量日志。流量日志表示为 $log=<Ps, Pr, Pf>$，其中

$$\begin{cases} Ps = N_{\mathrm{SP}} / \Delta t \\ Pr = N_{\mathrm{RP}} / \Delta t \\ Pf = N_{\mathrm{FP}} / \Delta t \end{cases} \tag{10}$$

N_{SP}、N_{RP} 和 N_{FP} 分别表示节点在$?\,t$时间内发送，接收和转发的网络数据分组的数目。在决策节点接收到危险域内所有节点的流量日志或者等待超时之后，决策节点停止收集，并提呈抗原。

受体是组成抗原和抗体的基本单元，每一个节点 i，都有一个 Id_i 和相对应的受体，受体表示为

$$R(Id_i)=<Id_i, Ps, Pr, Pf, \{NeighborList\}> \tag{11}$$

假设危险域有 k 个节点，抗原可以表示为

$$Ag=\{\bigcup_{i=1\sim k} R(Id_i)\} \tag{12}$$

3.3　决策

决策节点负责分析提呈的抗原，确认入侵行为的存在。

分析过程采用传统的自我-非我识别，通过计算抗原和抗体之间的亲和度确认是否发生了入侵。抗原通过对受体库进行免疫耐受过程产生。受体库为每个节点预定义的自我集合，仅存储在决策节点上。APC 激活了受体库，为每个节点提供数目为 m 的非我受体，非我受体组成抗原。

为了区别用于组成抗原和抗体的受体，使用

$\hat{R}(Id_i)$ 来表示耐受产生的非我受体。抗体表示为

$$Ab = \{ \bigcup_{i=1\sim k} \hat{R}(Id_i) \} \tag{13}$$

从式(13)可以看出，受体是组成抗原和抗体的基本单元，受体也是用来识别的基本单元。决策节点从抗原当中提取出 Id_i，并激活受体库产生抗原，分别将抗原与抗体中的受体使用亲和度函数。本文使用 Euclidean 距离函数来计算亲和力，对每个 Id_i，受体之间的距离为

$$A(Id_i) = \sqrt{(ps - \hat{ps})^2 + (pf - \hat{pf})^2 + (pr - \hat{pr})^2} \tag{14}$$

抗原和抗体之间的亲和力为

$$A(Ag, Ab) = \frac{1}{\sum_{i=1}^{k} A(Id_i)} \tag{15}$$

如果 $A(Ag, Ab) > ß$，则认为确实发生了入侵，$ß$ 为亲和力阈值。

图 3 描述了危险域中有 4 个节点的抗原和抗体的匹配过程，从图中可以看出 $R(Id_1)$、$R(Id_4)$ 与 $\hat{R}(Id_1)$、$\hat{R}(Id_4)$ 匹配度高，这就说明 Id_1 及 Id_4 节点为潜在的入侵者和严重受害者。

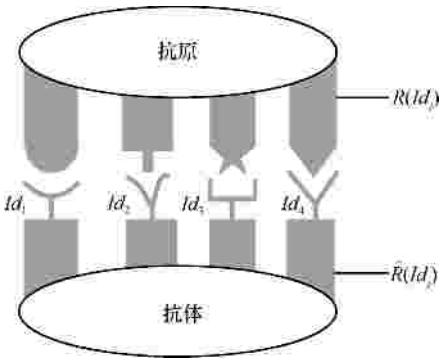


图 3　抗原、抗体亲和力匹配

自我受体库不应是静态的，而应是随着检测结果动态变化的，如可以通过记忆受体减低检测试验或者淘汰长时间没有用到的受体等，本文关注与整个检测模型的性能，对自我受体库的维护不做过多的讨论。

4　仿真实验及性能分析

通过仿真验证将危险理论应用到无线传感网络的优势，从检测率、误检率、能耗等方面分析检测模型的性能。本文采用基于离散事件的 OMNET++4.1 仿真器进行仿真。节点随机分布在网络当中，具体的网络参数如表 2 所示。

表 2　模拟实验参数

参数	默认值
网络部署区域大小/m²	1 000m×1 000m
节点通信半径 r/m	100
节点数量	300
MAC 层协议	IEEE 802.15.4
路由协议	Flooding
通信速率/(kbit·s⁻¹)	250
数据分组长度/byte	128
检测时间间隔 $?t$/s	60
非我受体个数 m	5
危险阈值 d	0.2
亲和力阈值 $ß$	0.3

图 4 给出了最终形成的仿真网络拓扑，随机选择攻击节点的位置。

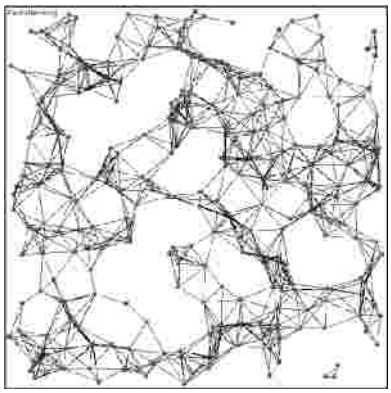


图 4　仿真网络拓扑

主要仿真包阻塞攻击，攻击节点每隔 60s 就向周围广播一个无意义的数据分组，以达到降低信道可用性及消耗周围节点能量的目的。首先采集 10 次正常情况下的数据以产生自我受体。对于每一种攻击节点数目{1,3,5,7,10,15}独立运行 10 次仿真，模拟持续 2 个小时网络的变化，结果取均值。

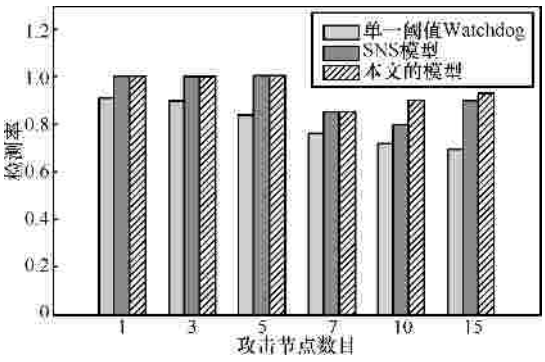
4.1　检测性能分析

将本文提出的模型与单一阈值 Watchdog 和 SNS 模型进行对比。单一阈值 Watchdog 采用文献[10]提出的 Watchdog 算法的基本思想，监听网络流量通过单一阈值判断是否发生入侵。SNS 模型采用文献[7]的检测方法，单个节点运行检测实例，通过自我-非我来判断是否发生入侵。

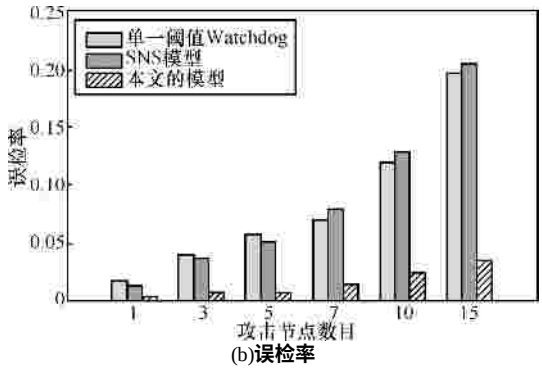
图 5 给出了在检测率和误检率方面的性能对比。从图 5(a)可以看出，采用了人工免疫思想的方法在检测率上具有更好的性能。当攻击节点数量比较少时，基于 SNS 模型的方法和本文提出的方法都能准确地检测到入侵，检测率为 1，当攻击节点数目多时，由

于本文提出的模型能够获得更加全局的信息，而不限于 2 跳范围内的流量信息（采用混杂模式监听），所以在检测大规模的入侵时，具有较好的检测结果。

在误检率方面，从图 5(b)可看出，采用单一阈值 Watchdog 的方法和 SNS 模型中节点通过将收集到的流量异常与正常流量相比较或匹配，发现异常就认为检测到入侵，而在基于危险理论的入侵检测中，存在 2 层检测确认，第 1 层是节点感知到危险，认为存在潜在的入侵，第 2 层是全局流量匹配确认，所以本文提出的方法有效地降低了检测系统的误检率。



(a) 检测率



(b)误检率

图 5 检测率和误检率对比

4.2 能耗分析

在单一阈值 Watchdog 和 SNS 模型当中，节点需要时刻处于混杂模式监听网络流量信息，一直有能量的消耗。而在本文提出的模型当中，节点只需在正常唤醒时处理感知自身的危险，在收到上传流量日志时上传自身的流量信息，没有过多的检测能量消耗。本文仿真了 TI CC2420 射频模块，节点电压为 3.3V，接收产生的能耗为 18.8mA，发送时的能耗为 17.4mA，睡眠时的能耗为 0.021μA。

传感器传输信息要比执行计算更消耗电能，研究表明，传感器传输 1bit 信息需要的电能足以执行 3000 条计算指令。所以主要考虑接收发送数据产生的能耗，而不考虑由于计算产生的能耗。能量消耗可以表示为

$$Cost=bitrate^{-1}\times n\times(Ns\times Is+Nr\times Ir)\times V \quad (16)$$

式(16)中参数 *bitrate* 为 250kbit/s，*n* 是每个数据分组的比特数为 128×8bit，*Is* 为 17.4mA，*Ir* 为 18.8mA，*V* 为 3.3V, *Ns* 和 *Nr* 为仿真结束时节点收到的发送和接收的数据分组的总和，与具体的网络环境有关，表 3 描述了不同攻击节点数目情况下，感知到危险节点数目，可以看出攻击节点越多，发出的危险信号越多，用于检测的数据分组越多，能耗越大。而对于采用监听模式的方法来说，每个节点都要捕获自己通信范围内的数据，所以能耗与网络通信流量直接相关。

图 6 描述了在重复 10 次实验取均值后的系统能耗比较。从图中可以看出，在攻击节点少的情况下，本文提出的检测模型具有明显优势，当攻击节点增多时，如表 3 所示，网络中感知到危险的节点增多，当出现 15 个攻击节点时，有 1/3 的节点发出了危险信号，这样由于抗原提呈产生的能耗也增大，系统能耗趋近于其他 2 种方法。所以在能耗方面，在受难节点数量不多的入侵环境当中，本文提出的模型具有明显的优势。

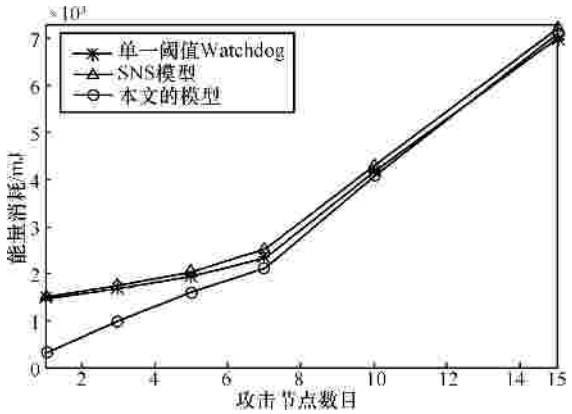


图 6 系统能耗

表 3 不同攻击节点数目情况下感知到危险的节点数目

攻击节点数目	感知到危险的节点数目
1	9
3	26
5	45
7	58
10	79
15	100

5　结束语

本文引进危险理论的基本工作原理，提出了一种适用于无线传感器网络入侵检测模型。与传统的基于 AIS 的入侵检测技术相比，本文提出的模型具有以下特点：1）只有感知到危险之后才对网络流量进行异常识别，危险感知过程基于本地知识不产生额外的通信开销；2）没有采用混杂模式获得全局的流量信息，引入了节点合作，不需要额外的唤醒节点收集信息；3）由于采用了分布式的合作机制，不需要在每个节点上都运行一个完整的检测实例，只有在中心节点上维护受体库和抗体进行流量的异常检测。结果表明，这 3 个方面大大降低了普通节点和整个网络的检测开销并提高了检测性能。

参考文献：

[1] KIM J, BENTLEY P, AICKELIN U, *et al*. Immune system approaches to intrusion detection-a review[J]. Natural Computing, 2007, 6(4): 413-466.

[2] YI P, WU Y, CHEN J L. Towards an artificial immune system for detecting anomalies in wireless mesh networks[J]. China Communications, 2011, 8(3): 107-117.

[3] MATZINGER P. Tolerance, danger and the extended family[J]. Annual Review Immunology, 1994, 12: 991-1045.

[4] WU S X, BANZHAF W. The use of computational intelligence in intrusion detection systems: a review[J]. Applied Soft Computing, 2010, 10(1):1-35.

[5] AICKELIN U, BENTLEY P, CAYZER S, *et al*. Danger theory: the link between AIS and IDS[A]. Proceedings of the Second International Conference on Artificial Immune Systems[C]. Edinburgh, UK, 2003. 147-155.

[6] KIM J, BENTLEY P, WALLENTA C, *et al*. Danger is ubiquitous: detecting malicious activities in sensor networks usin the dendritic cell algorithm[A]. Proceedings of the International Conference o Artificial Immune Systems[C]. Cambridge, UK , 2006.390-403.

[7] DROZDA M, SCHAUST S, SZCZERBICKA H. AIS for misbehavior detection in wireless sensor networks: performance and design principles[A]. Proceedings of the IEEE Congress on Evolutionary Computation, Special Session on Recent Developments in Artificial Immune Systems[C]. Singapore , 2007. 3719-3726.

[8] DROZDA M, SCHAUST S, SCHILDT S, *et al*. Priming: making the reaction to intrusion or fault predictable[J]. Natural Computing, 2011, 10(1):243-274.

[9] DROZDA M, SCHILDT S, SCHAUST S, *et al*. An immuno-inspired approach to misbehavior detection in ad hoc wireless networks[EB/OL]. http://arxiv. org/abs/1001. 3113, 2010.

[10] MARTI S, GIULI T, LAI K, *et al*. Mitigating routing misbehavior in mobile ad hoc networks[A]. Proceedings of the International Conference on Mobile Computing and Networking[C]. Massachusetts, USA, 2000. 255-265.

[11] SCHAUST S, SZCZERBICKA H. Applying antigen-receptor degeneracy behavior for misbehavior response selection in wi less sensor networks[A]. Proceedings of the 10th International Conference on Artificial Immune Systems[C]. Cambridge, UK, 2011.212-225.

[12] BALACHANDRAN S, DASGUPTA D, WANG L. A hybrid approach for misbehavior detection in wireless ad-hoc networks[A]. Proceedings of the Symposium on Information Assurance[C]. New York, USA, 2006. 14-15.

[13] **孙利民, 李建中, 陈渝等. 无线传感器网络**[M]. **北京: 清华大学出版社**, 2005.
SUN L M, LI J Z, CHEN Y, *et al*. Wireless Sensor Networks[M]. Beijing: Tsinghua University Press, 2005.

[14] RAO V P, MARANDIN D. Adaptive backoff exponent algorithm for zigbee(IEEE 802.15.4)[A]. Proceedings of 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking[C]. St Petersburg, Russia, 2006. 501-516.

作者简介：

傅蓉蓉（1987-），女，江苏盐城人，北京交通大学博士生，主要研究方向为自组织网络安全与人工智能算法。

郑康锋（1975-），男，山东烟台人，博士，北京邮电大学讲师，主要研究方向为网络与信息安全。

芦天亮（1985-），男，河北保定人，北京邮电大学博士生，主要研究方向为信息安全、人工智能与恶意代码检测。

杨义先（1961-），男，四川盐亭人，北京邮电大学教授、博士生导师，主要研究方向为信息安全和密码学。