doi:10.11959/j.issn.1000-436x.2015301

基于朋友机制的移动 ad hoc 网络路由入侵检测模型研究

肖阳，白磊，王仙
（西安电子科技大学 通信工程学院，陕西 西安 710071）

摘 要：从如何有效检测移动 ad hoc 网络路由入侵行为、如何准确地响应并将恶意路由节点移除网络，提供可信路由环境的角度进行分析，提出了一种基于朋友机制的轻量级移动 ad hoc 网络入侵检测模型，并以典型的黑洞攻击为例，通过 OPNET 网络建模仿真及实验分析，验证了该模型的可行性和有效性。
关键词：移动 ad hoc 网络；路由安全；入侵检测；朋友机制
中图分类号：TN929 **文献标识码**：A

Friends mechanism-based routing intrusion detection model for mobile ad hoc network

XIAO Yang, BAI Lei, WANG Xian
(School of Telecommunication Engineering, Xidian University, Xi'an 710071,China)

Abstract: The proposed model mainly focused on how to effectively detect routing invasions from mobile ad hoc network as well as how to accurately respond to the malicious nodes, providing a trusted routing environment. A lightweight intrusion detection model was proposed to based on the friends mechanism, taking black hole attack for example, the OPNET software gives the simulation test, and results show that the schemes can effectively detect attacks, it is validated and compared with other conventional models.
Key words: mobile ad hoc network; routing security; intrusion detection; friends mechanisms

1 引言

移动 ad hoc 网络是一种融合了无线技术、移动网络技术及对等通信技术的动态拓扑网络，被广泛地应用于诸如军事通信、抢险救灾等多种通信环境中。移动 ad hoc 网络本身具有的一些独特性使其不同于其他类型的网络，其无需借助任何基础设施，以自组织的方式分布式动态运行，使用无线链路进行通信。然而，和其他网络相比，正是由于其独有的特性给移动自组网带来节点间协作、路由、安全等多种新问题。其中，选择合适的路由及路由信息的维护是提供正常网络服务的基础，对网络拓扑的维护尤为重要。移动 ad hoc 网络中任何节点都可能参与路由，很容易遭受外部或内部的攻击，因此路由安全研究是移动 ad hoc 网络进一步发展的关键问题之一。作为入侵防御机制的加密、认证等技术虽然在自组网路由安全中广泛应用，但其都是针对于外部攻击，对来自网络内部的攻击却无能为力，这就需要将行为检测和响应技术与之互为补充，共同保障路由安全。

入侵检测系统作为一种网络安全工具，动态地监控网络中发生的事件并决定这些事件表征的是网络的正常行为还是恶意袭击，能够对已经转变为恶意节点或者新加入的恶意节点进行检测。近年来，无线入侵检测系统的提出成为一个新的研究话题，其目标在于开发一个新的架构和机制来更好地保护无线网络。但目前大多数的入侵检测系统研究集中在有线网络，而有线网络与移动 ad hoc 网络之间的显著差异使传统的 IDS 不能直接运用于无线网络，其大多数都采用集中式的入侵检测，由于移动自组网的自组织、无中心特点，分布式解决方案成

收稿日期：2015-10-27
基金项目：国家自然科学基金资助项目（61373170）
Foundation Item: The National Natural Science Foundation of China (61373170)

为主流，其系统架构主要有单点式孤立 IDS、分布式协作 IDS 和层次化 IDS 这 3 种，现有的大多数入侵检测方案，如基于规范(specification-based)的分布式协作入侵检测[1]、基于分组丢失和路由表异常变化的入侵检测[2]、基于智能代理和数据挖掘技术的入侵检测[3]、基于贝叶斯网络的层次 ad hoc 网络入侵检测方案[4]等都是基于这些模型提出的，通过对这些方案深入的研究分析，发现其在不同程度上都有各自的缺陷和不足，但对解决移动 ad hoc 网络的安全问题起到了不同程度的效果，为移动 ad hoc 网络中入侵检测技术的进一步研究提供了较好的依据。

通过参考已有的移动 ad hoc 网络入侵检测模型和方法，针对移动 ad hoc 网络的无中心、自组织、动态拓扑、能量有限等特性，本文主要从入侵检测系统的 2 个方面进行讨论，即如何有效检测移动 ad hoc 网络路由入侵行为、如何准确地响应并将恶意路由节点移除网络，提供可信路由环境的角度进行分析，提出了一种基于朋友机制的轻量级移动 ad hoc 网络入侵检测模型。

2 相关理论

基于对上述提及的入侵检测方案模型的研究分析，下面针对移动 ad hoc 网络环境入侵检测系统架构的设计总结出以下经验，以此来指导本文的入侵检测系统框架设计工作。

1) 层次化，即 IDS 必须能对每个节点进行入侵检测，节点必须能协作完成是否发出警报的决策。

2) 具有通用性，不依赖于特定的路由协议。

3) 不仅能阻止特定类型的攻击，对于未定义的攻击也可以检测阻止。

4) 能够自适应、易于配置，而不会增加过多的开销，保证 IDS 消耗的资源应最小化。

5) 需要选取合适的统计特征值，使其能够处理异常与正常行为之间没有明确界线这样一个问题，最大化地降低误判率，提高检测率。

2.1 支持向量机

在处理实际问题时，由于传统的统计学是基于样本数目趋向于无穷大时的渐进理论，因此针对样本数量有限的实际环境，像神经网络中的 BP 算法等这些优秀的统计学习方法却不尽人意。于是，在统计学习理论的基础上，出现了一种新的学习理论，即支持向量机(SVM，support vector machine)。SVM 用于解决各种学习、分类和预测问题，由 Vapnik 等[5]于 1995 年在 《The Nature of Statistic Learning Theory》一书中提出。借鉴众多研究者将 SVM 运用到移动 ad hoc 网络入侵检测系统中的经验：SVM 用于入侵检测时能够提供很高的检测正确率；通过特征值的选择来降低算法复杂度，使 SVM 在有限资源的 ad hoc 网络中可以保持很好的检测性能；SVM 能够解决训练样本获取代价过高带来的问题。因此，本文提出的入侵检测模型也将 SVM 作为网络入侵行为的识别算法。

1) 核函数

核函数在支持向量机中扮演重要的角色，选择不同的核函数将生成不同的算法。在实践中，根据输入数据集的复杂性可以使用多种内积核函数，如线性内核、多项式内核、径向基内核和 Sigmoid 内核。

①线性核函数

$$K(x_i,x_j)=x_ix_j \tag{1}$$

②多项式核函数（以下是 q 阶多项式分类器）

$$K(x_i,x_j)=[(x_ix_j)+1]^q \tag{2}$$

③径向基核函数(RBF, radial basis function)

$$K(x_i,x_j)=\exp\left\{-\frac{|x-x_i|^2}{\delta^2}\right\} \tag{3}$$

其中，x_i 为核函数中心，δ 为函数的宽度参数，控制了函数的径向作用范围。

径向基核函数就是某种沿径向对称的标量函数。每个函数中心对应一个支持向量，向量及其对应的输出权值都是由算法自动确定的，这与传统 RBF 方法有重要区别。最常用的径向基函数是高斯核函数。

④Sigmoid 内核，也称作 S 形内核

$$K(x_i,x_j)=\tanh(v(xx_i)+c) \tag{4}$$

2) SVM 的训练算法

Vapnik 等[5]将 SVM 的训练归结为解一个凸二次优化问题，SVM 中的其他问题，如确定核函数中的参数或者惩罚系数，也常归结为此类优化问题。一般采用循环迭代的方法，把原来问题分解为若干个子问题来求解，使最终结果收敛到原问题的最优解。根据子问题的划分和迭代策略分为“块算法”和“分解算法”2 类。

Platt[6]提出的 SMO(sequetial minimal optimizaton)方法作为“分解算法”的一个特例，对大训练样本问题进行了解决，能有效避免多样本下的数值

解不稳定和耗时问题，不需要很大的存储空间，而且算法速度快。

Keerthi S S 等[7]在 Platt 提出的 SMO 算法的基础上进行了改进，使算法更加有效合理。

Joachims[8]对“分解算法”和 SMO 算法进行了具体的编程实现，将其集成在 SVMLight 软件包中，能较好地处理大规模训练集问题。

林智仁等[9]对 SMO 算法和 SVMLight 软件中的工作集选择方法进行综合，采用 C++设计实现了一个简单、易于使用和快速有效的 SVM 模式识别与回归的软件包 LIBSVM。它不但提供了编译好的可在 Windows 系列系统地执行文件，还提供了源代码，方便改进、修改以及在其他操作系统上应用。该软件对 SVM 所涉及的参数调节较少，一般利用提供的大量默认参数就可以解决很多问题，并提供了交互检验(cross validation)功能，使 LIBSVM 作为 SVM 训练工具使用最为方便。第 4 节在对黑洞攻击模型获取的原始数据训练测试中正是使用了 LIBSVM 软件工具。

2.2　朋友机制

2.2.1　基本概念

早在 1967 年，哈佛大学的心理学教授 Milgram[10]通过实验证实了“小世界现象”的存在，简而言之，就是在任何地方随机地选取任意 2 个人，他们之间经过一条不超过 6 个熟人的链连接，也就是说最多通过 6 个人你就能够结识任何一个特定的陌生人，因此也被称作“六度分割理论”。后来有一些研究人员拓展了他的这种理论，他们认为在某种程度上万维网也是一种“小世界”，并将其扩展到了互联网应用，即所有的网站是高度集群化的并且它们之间的路径长度很小。Helmy[11]通过仿真实验进一步建立了小世界概念和无线网络之间的关系，然而并没有讨论如何将这种关系有效地运用于系统中。后来，Capkun 等[12]基于“小世界现象”提出 friendships 机制，并将“friends”的概念引入到具有自组织、分布式特性的移动 ad hoc 网络中来解决许多问题，尤其是安全相关的问题。建立节点之间的朋友关系类似社会学中的朋友关系，研究人员做出以下假设：移动 ad hoc 网络中的任意 2 个节点在成为朋友之前必须相互认识，即能够直接通信，其次互相信任，这类节点称之为“一度朋友”或者“直接朋友”。对于不能直接通信的节点，如果它们有共同的一度朋友，那么这类节点称之为“二度节点”或者“间接朋友”。具体场景如下。一对节点，在加入网络之前假定它们之间互相信任，则它们能够在网络通信过程中建立安全关联，通过这种安全关联根据朋友节点之间直接或间接的信任评价能够加速网络中节点可信域的产生过程，从而减少了节点的匿名不安全通信。

2.2.2　朋友机制在移动 ad hoc 网络中的应用

近年来朋友机制以其优越性广泛地用于多种网络及其安全性问题的研究。裴伟东等[13]在研究复杂网络模型时，从“朋友”机制捕捉网络形成的动态特性，了解该机制对网络最终结构的影响，提出了一种新的无标度网络演化模型。马春娥等[14]在基于移动 ad hoc 网络安全性模型研究中利用“朋友”机制，提出了一种在移动节点“临近”的时候，建立移动节点间安全关联的机制，有效地对节点间建立安全关联的步长进行了评估和建模仿真。另外，朋友的概念被用于防止路由机制中节点的自私行为。在 MANET 中，有的节点为了保护自己有限的资源拒绝加入路由转发。如文献[15]所述，一般通过 2 种方式强制这类节点参与网络操作，即要么对他们的不合作行为进行惩罚，要么奖励他们的参与。然而，这种机制会产生不公平，特别是对于那些处于通信繁忙区域之外的节点。节点依赖自身的信用值在网络中发送其数据分组，而信用值的积累仅仅是在转发其他节点数据分组时获得。然而，对于处于通信繁忙区域之外的节点，在数据分组转发的过程被选择的机会相对较低，这将使他们很难获得更多的信用。Miranda 等[16]提出用“朋友”的概念来解决这个问题。他们建议路由过程使用选择性转发，其中每个节点将只参与一个数据分组的转发过程，如果数据分组是来自或者需要被发送到它的一个朋友节点，节点将推荐给它朋友列表中的其他节点，从而避免其被指控为不转发其他不是朋友节点的数据分组。

3　基于朋友机制的轻量级入侵检测模型

3.1　相关假设

网络系统的安全性研究往往依赖于一些特殊的假设，以确保其有效性和简单性。为此，本文从以下 3 个方面进行约定。

1) 直接朋友机制（DFM, direct friend mechanism）

首先，在入侵检测系统执行的最开始，考虑移

动 ad hoc 网络中有 5 个节点，假定每个节点可信任的初始节点列表，被称为直接朋友机制，如表 1 所示。此时，由于每个节点对其他节点不可能有足够的经验，因此无法给出正确的评估，则认为彼此是零知识的朋友关系，即不考虑其他节点的推荐信任（这种假设是可行的，则在组网之前用到的所有节点都会是可信的，而之后由于拓扑变化及节点的妥协等因素引入的恶意节点，就交给入侵检测系统来处理）。另外，朋友列表被网络中的其他可信节点所共享，并且节点的初始信任列表根据图 2 所示的全局朋友轮廓数据库进行更新，产生新的朋友集，即间接朋友关系。

表 1　　节点初始信任关系

节点	初始信任节点
A	B,C
B	C,D,E
C	A,D,B
D	C,B
E	A,C

2) 入侵检测预警分析

在入侵检测模型设计之前，讨论其预警分析的结果是非常有必要的。根据审计的流量踪迹入侵检测的预警分析通常有 4 种可能的结果。

TP(true positive)：攻击成功并且 IDS 能够检测出来。

TN(true negative)：攻击没有成功并且 IDS 没有报告。

FP(false positive)：没有攻击但是 IDS 给出报告。

FN(false negative)：攻击成功但是 IDS 没有检测出来。

其中，TP 和 TN 是正确的预警响应，它们有助于提高入侵检测系统的精确性；而 FP 和 FN 则是影响误报和漏检的主要因素，降低入侵检测的准确性。

3) 入侵检测系统的准确性

检索率(recall)是指通过搜索从数据库中能够获取的所有相关文件占总的文件百分比[17]。如果用户已知数据库中有 1 000 个相关文件，而通过搜索只能获得 100 个相关文件，这时检索率就是 10%。这里主要是指攻击成功后能够正确检测到的攻击行为比率。即

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

精确度(precision)是指获取的相关文件数占获取的所有文件数目百分比[17]。假设获取到 100 个文件而相关联的文件仅有 20 个，那么精确度为 20%。这里主要是指已经报告为攻击行为，而确实属于攻击行为的比率。即

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

基于上面 2 个参数的讨论，给出综合评价入侵检测系统识别攻击行为准确性的公式，即

$$IDS\text{准确性} = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

式(7)计算结果值的高低最终决定了所设计的入侵检测框架性能的好坏与否。

3.2 入侵检测系统模型详细设计

本文提出的入侵检测系统模型主要由 2 大模块组成，分别是本地入侵检测模块和全局入侵检测模块。其中，本地入侵检测位于第一层，由于其能够收集获取到网络局部的一手信息，对任何的可疑活动可快速检测，而全局入侵检测过程需要较长时间来完成，这是因为更多全面信息的获取要通过其他可信节点来提供，时间相对较长。同时，为了提高本地入侵检测模块的检测率及响应速率，即尽可能地在系统前期检测出入侵行为，使攻击危害最小化，那么在设计入侵检测模型时，使其遵守 20:80 定律将会大大提高入侵检测的效率。这里主要是指检测引擎规则的比例设置基于二八原则的概念，即在本地入侵检测模块中将规则的 20%设定为高检测阈值，一方面它能够快速地检测出节点的异常行为活动，另一方面，使本地入侵检测模块生成的朋友列表也相对较快。然而，降低检测阈值的时候检测率提高，误报率势必也会提高，为尽量减小误报率，在响应模块进行约定，本地响应模块只对来自其直接朋友的报警才发出警告，否则进入全局检测模块做进一步的检测。而在全局入侵检测模块，设置正常的入侵检测阈值规则对本地入侵检测模块中未检测到的异常行为进一步过滤、识别，并通过全局朋友机制进行更为全面、严格的检测。

本地入侵检测模块和全局入侵检测模块又分别由许多个小部件构成，下面将对这 2 大模块的设计细节进行详述。

3.2.1　本地入侵检测模块设计

本地入侵检测模块由 5 大部件组成，分别是数据收集模块、本地检测引擎模块、本地入侵响应模块、本地用户轮廓数据库、全局入侵检测引擎接口模块，如图 1 所示。

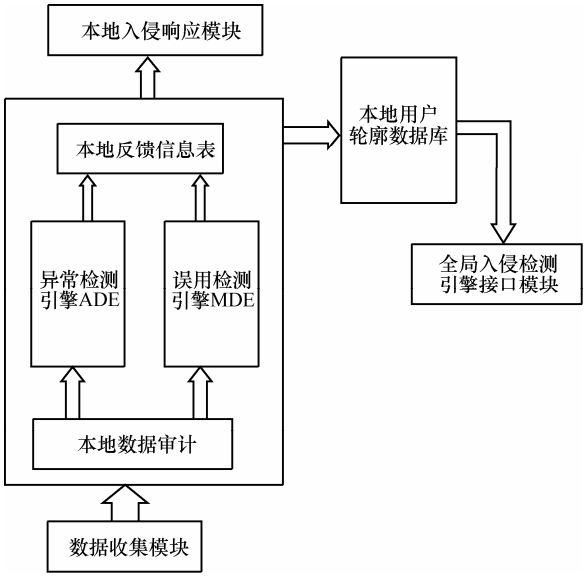

图 1　本地入侵检测模块

数据收集模块的功能是收集来自于不同监控数据源的（一般分为基于主机的审计日志和基于网络的数据报文）与安全相关的数据，并根据检测引擎的需求格式进行格式转换等预处理。由于基于主机的数据源不依赖于任何网络结构，应用在有线网络中的数据收集技术完全可以用于移动 ad hoc 网络。例如，可以使用简单网络监控协议 SNMP 来记录用户的行为活动或者使用代理机制收集有用的数据源。但是，由于移动自组网的无中心、自组织特性使有线网络中基于网络的数据源收集技术不能直接用于移动 ad hoc 网络，根据移动 ad hoc 网络的无线通信特性，任意节点可以采用监听模式捕捉到它周围邻居节点的网络活动，只不过这些数据源是局部的。另外，由于收集到的源数据往往夹杂着噪音等无用信息，应对这些实时数据汇聚精简，做过滤、降噪处理，同时还要提取出主要特征信息、预处理转化为检测引擎的输入格式。这部分可以采用诸如机器学习算法、神经网络算法、模糊算法、数据挖掘算法等技术来实现。本文主要研究的是网络层的路由安全，即考虑的数据源主要包括网络中的路由活动、拓扑模式及通信的变化情况等。

本地检测引擎可以根据模块中已经存在的网络正常轮廓、规则库等对数据收集模块收集处理后的数据源进行匹配，以识别当前网络是否存在攻击行为，也可以对节点的活动审计分析，抽取能够反映攻击特性的特征值。针对移动 ad hoc 网络的特性，模型设计中将误用检测和异常检测相结合并行使用，不但根据误用检测技术能有效快速地定位、检测已知类型的攻击，提高检测效率，而且利用异常检测技术通过分析攻击所具有的行为特征，训练和学习形成攻击模型，能够最大限度地检测到未知的网络入侵行为，降低漏检率。当 2 种检测技术的检测结果同时为可信节点时（这里假定其值均为 0），认为是朋友，将检测结果存入本地反馈信息表，如表 2 所示，同时经由本地用户轮廓数据库发送到全局检测引擎做进一步的核查。否则，将异常入侵行为信息提交到本地入侵响应模块，本地入侵响应模块针对其攻击行为做出响应。

表 2　　本地反馈信息

误用检测引擎 MDE	异常检测引擎 ADE	MDE^ ADE	状态
1	0	1	Intruder
0	1	1	Intruder
1	1	1	Intruder
0	0	0	Friend

本地入侵响应模块的功能是对本地入侵检测引擎检测的不可信行为按照前述约定的响应策略在本地网络内进行广播，避免攻击范围的进一步扩大，使其危害最小化。

本地用户轮廓数据库的功能是根据本地反馈信息表来维护可信邻居列表，即朋友关系列表，不可信节点将被移除网络。

全局入侵检测引擎接口模块的功能是连接本地 IDS 和全局 IDS，将本地入侵检测产生的朋友关系列表发送到全局入侵检测模块对可信节点做进一步严格的审查。

3.2.2　全局入侵检测模块设计

类似地，全局入侵检测模块由 4 大组件组成，分别是全局数据收集模块、全局检测引擎模块、全局入侵响应模块、全局用户轮廓数据库，如图 2 所示。

全局数据收集模块的功能是接收来自本地入侵检测模块汇总的相关数据源，包括本地数据收集模块收集及处理后的审计数据和本地 IDS 生成的朋

友关系列表。不需要重新执行数据收集、处理工作，降低了系统的复杂性。

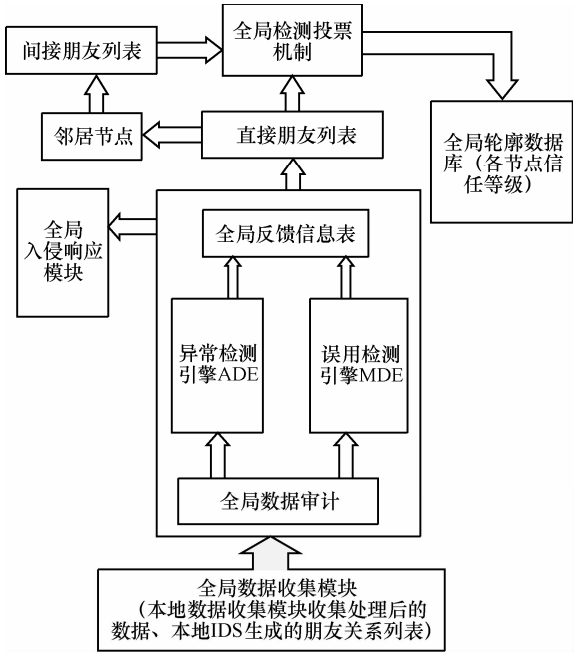

图 2　全局入侵检测模块

全局检测引擎模块的功能和本地检测引擎类似，不同之处在于此时的检测基准和阈值设定为入侵行为的正常水平，从而对上述数据源做进一步的检测审核。除此之外，生成更为精确的全局反馈信息表和最终的直接朋友列表，同时由本地 IDS 产生的可信邻居列表根据节点之间的信任关系生成间接朋友列表，通过综合来自直接朋友和间接朋友提供的信息来加速整个检测过程。最后由直接朋友列表和间接朋友列表中的节点各自以 0.5 的概率采用投票的方法加权计算出每个节点的最终信任级别。结合表 3 中给出的节点初始信任关系，全局检测模块最终根据其生成的直接朋友列表和非直接朋友列表产生每个节点的信任级别，如表 3 所示。

表 3　　节点的信任等级

节点	信任等级
A	2/5
B	3/5
C	4/5
D	2/5
E	1/5

全局入侵响应模块的功能是对全局入侵检测引擎检测的不可信行为按照响应策略在全局网络进行广播。这些不可信行为一般比较隐蔽，应加强检测引擎规则的分类和特征值提取技术，避免其造成更多的攻击。

全局用户轮廓数据库的功能是存储全局检测引擎生成的节点信任等级表，此表可用于移动 ad hoc 网络的可信路由选择和任何需要保证机密性的可信环境中。

3.3　入侵检测实现流程

本文提出的入侵检测模型的基本流程如图 3 所示。

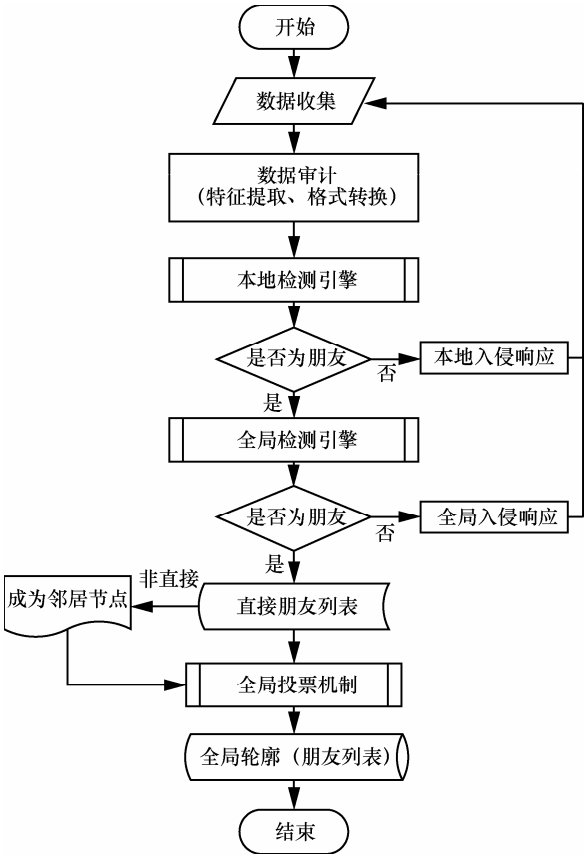

图 3　入侵检测流程

1) 数据收集模块主要获取基于网络的数据源，根据安全需求可以在网络各层，包括数据链路层、网络层、传输层等配置不同的监视器，获取入侵检测所需的原始数据，对检测模型进行实时反馈。

2) 数据审计模块可以采用统计学习、数据挖掘、模糊算法等技术将原始数据抽象为统计变量集，同时预处理转化为检测引擎的输入格式。

3) 本地检测引擎模块通过配置不同的检测技

术来实现，本文在检测引擎模块使用基于支持向量机 SVM 的异常检测算法。将上述生成的审计数据作为输入来运行 SVM 算法进行训练和测试，通过对攻击特点的分析，从训练数据集中识别出异常实例，建立一个区分正常数据和异常数据的分类边界，根据本文检测目标，选择相关的网络统计量作为特征参数，并将其统计值与当前设置的检测阈值比较，判断其是否有攻击行为，并初次检测可信任节点。

4) 如果第 3）步中检测引擎未检测出异常行为，那么认为是可信任的朋友节点，更新朋友关系列表，等待下一步的审核。否则，认为是可疑节点，并根据此节点的直接朋友反馈判断其是否为真正的恶意节点，如果是，就向本地响应模块发出入侵报警，进行本地广播，同时将此节点移除网络；如果不是，返回到第 1）步继续新一轮的检测。

5) 全局检测引擎模块对本地检测引擎初次检测的可信任节点和本地已经处理的审计数据做进一步更为全面、严格的检测，此时需要根据直接朋友节点和间接朋友节点各自的推荐信息来协作来判断，对恶意节点行为检测更为精准。尤其是这里的全局朋友机制对本地检测模块无法检测的欺诈攻击和恶意节点的共谋攻击可以有效抵御，克服了某些节点的不可信行为。

6) 如果第 5）步中判断有恶意行为，向全局响应模块发出预警；否则认为是朋友节点，并根据直接朋友列表判断其是直接朋友还是间接朋友，以此来更新相应的朋友列表。

7) 全局投票模块通过直接朋友和间接朋友之间的关系对各个节点投票，以此决定出每个节点最终的信任等级。

8) 全局朋友轮廓模块对所有的可信任节点存储，并标明其对应的信任等级，此时任何恶意节点或不可信节点将排除在此轮廓外，以便于后续安全路由的选择等。

最后，特别要注意的是，为了避免共谋节点的联合诬告攻击，减少误报率。对响应模块做出响应时设立以下规定：即本地或全局响应模块只对来自其直接信任朋友的报警才发出警告，广播给网络中的其他节点。

3.4　系统特点分析

通过对上述入侵检测模型各模块设计及具体检测流程的分析，可以看出，和目前已有的移动 ad hoc 网络入侵检测系统相比，本系统具有如下的特点。

1) 层次化结构。本系统采用两层式的入侵检测模型，通过对位于第一层的局部检测引擎设置二八准则，使其在系统检测初期能够最大化地检测出恶意攻击，从而使攻击危害最小化。对于本地引擎未能检测出来的可疑行为将进入位于第二层的全局检测机制做更为全面的检测，全局入侵检测机制则通过朋友节点的协作来判定节点的入侵行为。这种层次化结构的入侵检测系统在整个入侵检测过程中起到了加速检测的作用，可以提高检测速度，降低检测时间，有效地节省了节点的资源开销。此外，缩短了恶意节点在网络中的驻留时间，提高整个网络的安全性。

2) 朋友节点。全局检测机制需要其他朋友节点的协作，但是对于移动 ad hoc 网络这种特殊的网络环境，节点除了自身外不会信任其他任何的节点。为了有效解决节点间的信任问题，该模型引入朋友节点的概念，将网络中的其他节点分为一度朋友节点和二度朋友节点，一度朋友节点即完全可信任节点，二度朋友节点即间接朋友，需要中间的裁判节点对其身份进行确认才能得到信任。这样，通过节点间的互通合作关系有效地抵御了节点间各持己见引起的决策权问题及网络中自私节点和共谋欺骗节点的恶意行为，提高了系统检测的可靠性。

3) 轻量级。本文基于朋友机制设计的层次化入侵检测系统，和文献[18]中的入侵检测模型相比，它不需要签名管理、信任管理和入侵检测引擎预定义等复杂技术的支持，通过混合使用支持向量机算法和朋友关联机制，快速高效地从大量冗余数据中选择出相关性特征，系统计算资源消耗较低，实时性强，灵活性高，非常适合移动自组织网络环境。

4　建模仿真与分析

移动 ad hoc 网络路由安全中，最常见的攻击类型便是黑洞攻击。下面结合移动 ad hoc 网络自身的特点，在 OPNET 网络仿真环境下，以广泛使用的 AODV 协议为研究实例，在对黑洞攻击特点进行研究的基础上，分析讨论其攻击特征，并按照入侵检测流程对第 3 节中提出的基于朋友机制的入侵检测模型进行模拟实现。

4.1　黑洞攻击

黑洞攻击是一种借由丢弃封包的阻断服务攻击，这种攻击可以是选择性的或者成批的。通常在

路由发现阶段，恶意节点在收到源节点发送的 RREQ 请求分组后，通过伪造一个比目的节点更大的序列号来抢先快速应答，并声称其具有到目的节点的最短路径，将自己推荐给源节点，源节点误以为路由发现过程完成而忽略其他节点发送的 RREP 消息，选择了来自恶意节点的路由，从而改变正常的路由表。这将导致其他节点发送的数据分组都要经过恶意节点，恶意节点拦截经过自己的所有数据分组，形成了一个吸引数据的“黑洞”。

AODV 协议中的黑洞攻击过程如图 4 所示。S 想要向 D 发送数据分组进行通信，即发出 RREQ 分组进行最新的可用路由发现，恶意节点 A 接收到请求后，伪造一个比目的节点 D 的序列号更大的序列号，发送虚假路由信息给 S，并称其有最佳的路由（相比其他节点控制开销少或经过的跳数少），而实际中此节点可能根本无法到达节点 D。源节点选择图中经过恶意节点 A 的路由并开始数据分组的发送，攻击节点 A 通过反复对来自不同源节点的数据信息吸收，轻而易举地骗得大量的网络数据信息等，以极低的代价对网络造成严重的威胁。

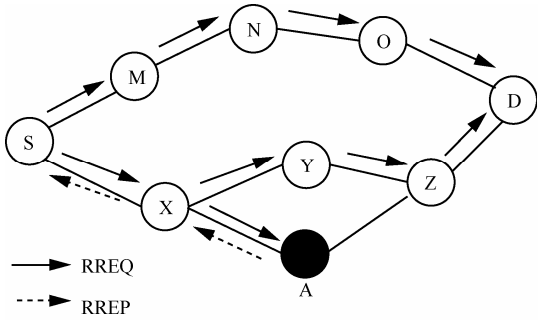

图 4 黑洞攻击原理

4.2 黑洞攻击检测方案

4.2.1 黑洞攻击仿真网络环境

为了有效获取黑洞攻击下的关键网络参数，使用 OPNET14.5 作为网络仿真平台，下面对移动自组网实验网络在 OPNET 环境的输入输出参数设定做一些说明。

实验中的通信信道设置为 ad hoc 模式，采用 802.11b 通信协议，每个节点的传输功率设为 0.005 W。模拟网络由 21 个移动节点组成 1 000 m×1 000 m 的运动区域，节点采用预设的随机路点轨迹 trajectory-5 (random way point)以(0~20) m/s 之间的速率随机移动，每一次的模拟时间为 3 600 s。其中，节点 20 作为目的节点，其他节点都向它发送路由请求，仿真环境如图 5 所示。

实验中，应用 AODV 路由协议，分别对正常情况和存在黑洞攻击的重要参数进行分析。

第一次仿真时不加入恶意节点，接下来将节点 6 换成恶意节点实施黑洞攻击，这样，通过多次仿真可以观察到网络的多种不同特征，由于本文的重点在于入侵检测系统性能的研究，这里主要对几个明显反映黑洞攻击特点的网络参数进行了仿真统计，进而可以对有无恶意节点情形下系统的性能做比较。

从图 6 和图 7 的仿真结果很容易分析出：网络中存在黑洞攻击时，虽然目的节点为节点 20，然而恶意节点 6 吸收了大部分的数据流量，导致路由过程中实际的数据流量转发效率很低，使整个网络的丢失分组现象非常明显。

4.2.2 黑洞攻击特征参数及其门限值的识别

1) 特征参数提取

为了区分节点的正常和入侵行为，进一步识别攻击，获取一些具体的特征值是必要的。基于 4.2.1 节的仿真实验，黑洞攻击的典型特征被加以提取，进一步可以验证黑洞攻击下本文提出的入侵检测系统的准确性。将图 6 和图 7 产生的原始统计数据导出到电子表格中进行特征分析，并对这些特征数据抽取预处理分类，然后在 Windows 64 bit 平台中的 LIBSVM 软件环境下，对处理后的数据按照黑洞攻击的以下 3 种特征：路由流量接收率、路由流量发送率和路由分组丢失率进行训练和测试。这 3 种特征参数的具体含义如下。

路由流量接收率（RRTR）

$$RRTR=\frac{\text{恶意节点接收的物总数据分组流量}}{\text{发送的总的路由数据分组流量}}$$

路由流量发送率（RRTS）

$$RRTS=\frac{\text{恶意节点发送的路由数据分组流量}}{\text{恶意节点接收的总数据分组流量}}$$

路由分组丢失率（RPD）

$$RPD=\frac{\text{恶意节点丢弃的数据分组}}{\text{路由过程中丢失的总的数据分组}}$$

2) 特征参数门限规则约定

通过上面利用 LIBSVM 软件对提取出的特征参数进行训练和测试，必须进一步估算和确定这些重要参数的门限值，这样通过对这些特征参数值的计算，并且和给定的门限值进行比较来判断各个节点所处的状态，为后面利用朋友机制检测提供依据。

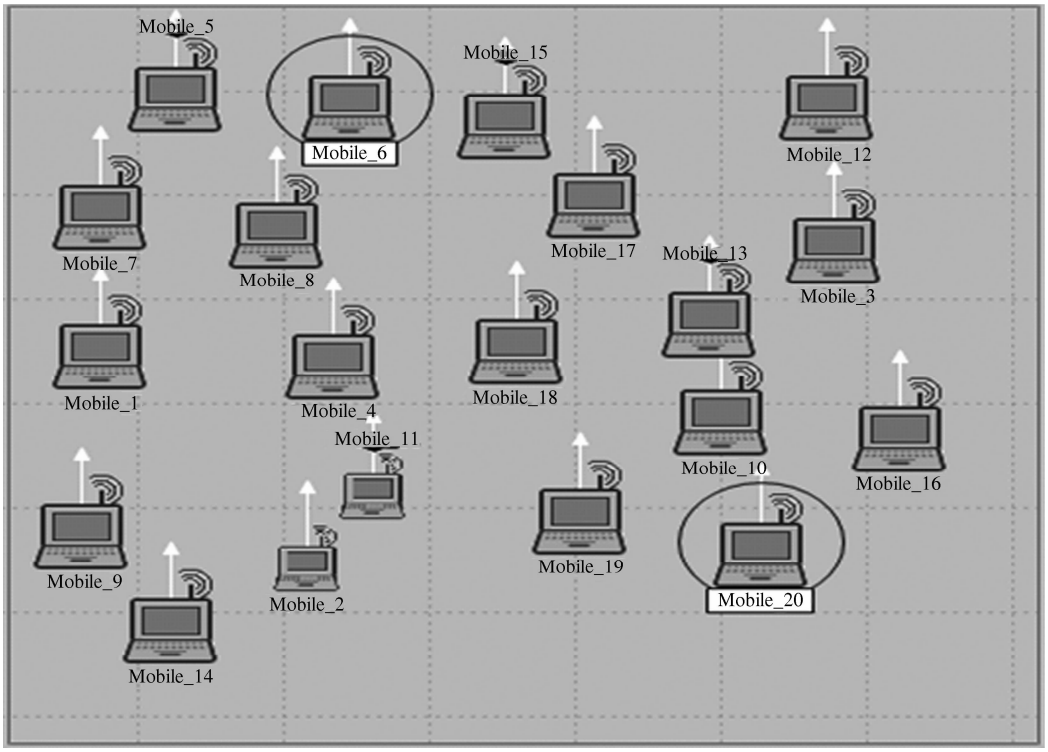

图 5　黑洞攻击仿真网络场景

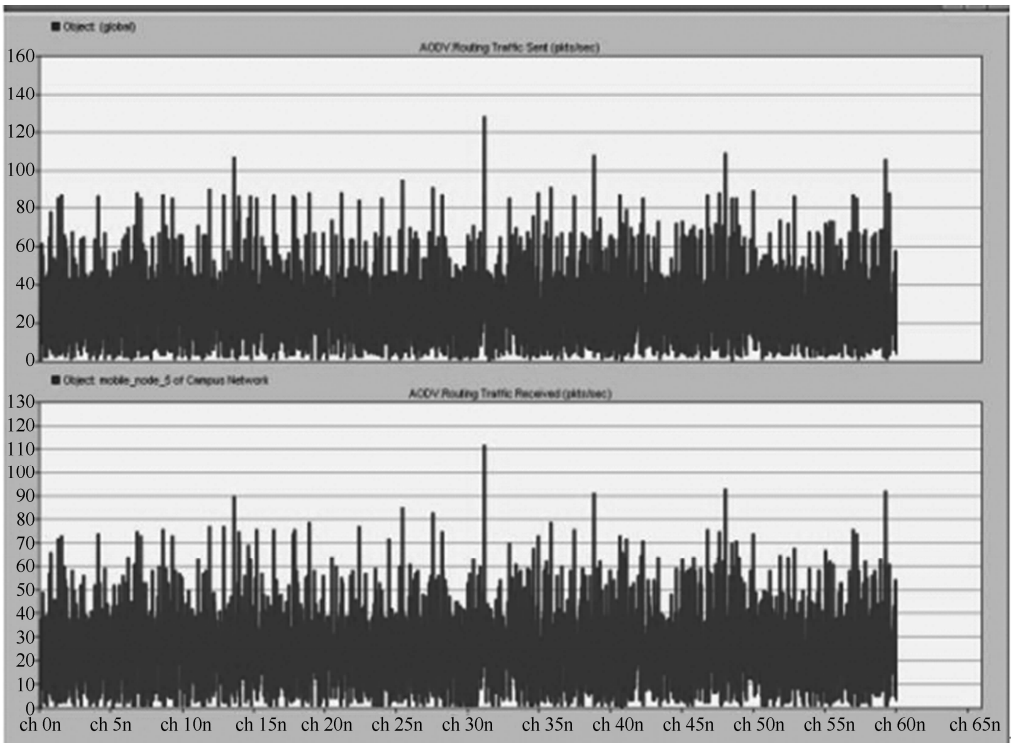

图 6　网络发送的总流量与恶意节点接收的总流量

在门限值识别实验中，将上述生成的黑洞攻击特征参数训练结果输入到 Matlab，根据曲线变化得到各个参数的门限值。如果一个节点的特征参数满足，那么可以判断该节点不是朋友节点。

约束条件如下。

If ((*RRTR* > 50% ^ *RRTS* < 10%) *PDR* >40%)

Then

{Not A Friend};

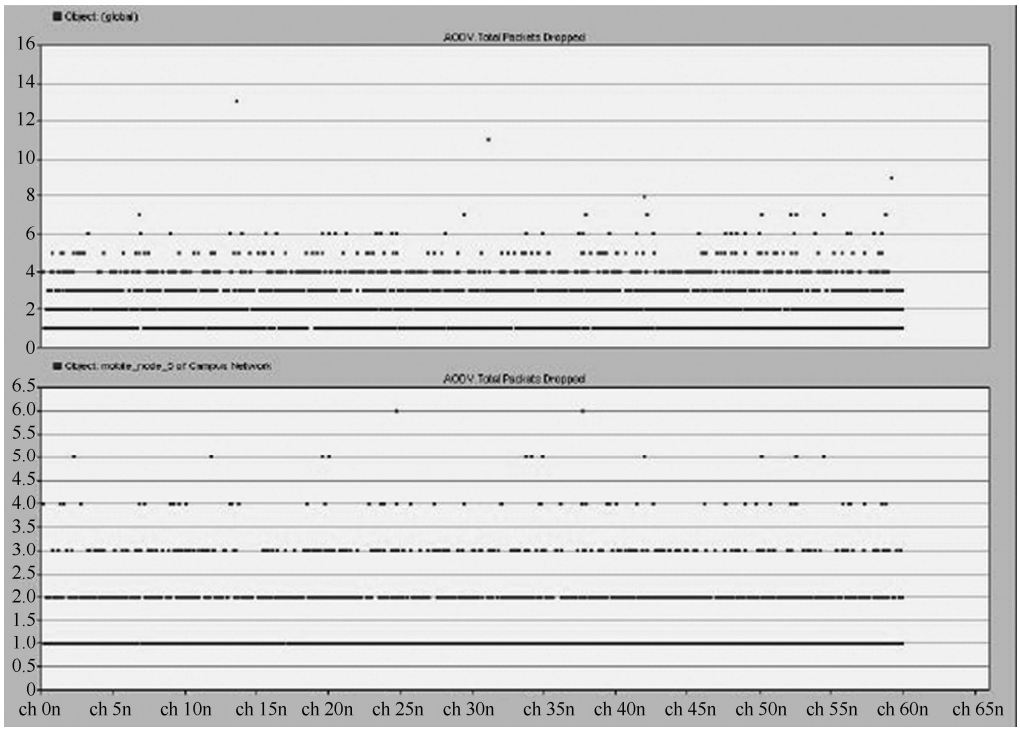

图 7　网络中丢弃的总数据分组与恶意节点丢弃的数据分组

这里强调的是，上述门限值是根据前面设置的仿真参数进一步实验得到的，不是对所有的移动 ad hoc 网络都有效，但在不同的网络需求中通过类似实验可以得到不同的门限值。

4.2.3　仿真结果

下面将使用 2.1 节中介绍的 LIBSVM 软件进行仿真。其中，拥有 3 568 个正常、怀疑和威胁状态的原始数据样本集、提取出 3 种重要的特征参数和约定好的门限值作为入侵检测框架的输入，通过改变 SVM 算法的核函数及同一个核函数中选取不同的惩罚因子 C 和核参数 γ 进行具体的实验。

1) > svm-train ../heart_myscale　train.model.text 其中，heart_myscale 表示输入的样本文件，train.model.text 表示生成的模型文件，如表 4 所示。经验证后，此模型文件可以部署在移动 ad hoc 网络节点模型中的网络 IP 层。移动 ad hoc 网络的节点模型如图 8 所示。

2) >svm-predict ../test.text　train.model.text output.text

本步骤将根据上一步中生成的模型文件对给出的测试数据样本进行预测，测试结果用于判断一个节点是正常节点还是入侵节点，如表 5 所示。

4.3　系统性能比较分析

从 4.2 节对黑洞攻击的测试数据实验结果可以

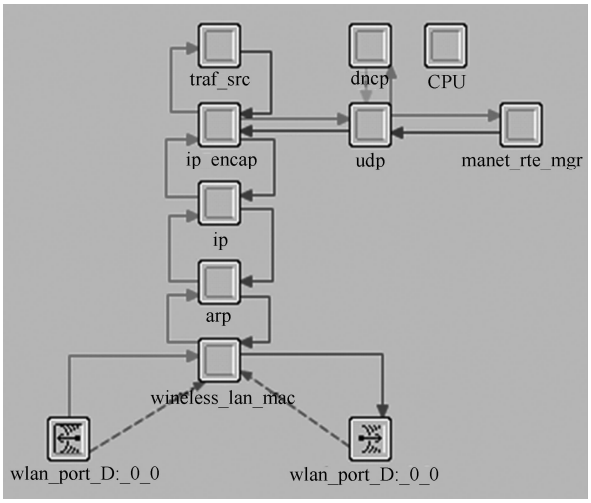

图 8　移动 ad hoc 网络的节点模型

看出，本文提出的检测模型在给定的朋友机制框架下对于不同的核函数系统检测的准确性差异较大，并且对同一个核函数设定不同的 C 和 γ 参数时，检测结果也会随之变化。通过对比可以发现：黑洞攻击下系统检测的准确性都是在取惩罚因子 C=2.0 及核参数 γ =1.0 时的径向基核函数表现得最好，系统检测的准确性分别高达 98.99%和 99.92%，那么完全可以通过在检测引擎中配置产生的这 2 种模型文件使本文提出的朋友机制检测模型具有较高的检测性能。为了验证本文提出的入侵检测系统的有效性，进一步对该模型下

表 4　　黑洞攻击训练模型数据

输入特征参数个数	数据样本	核函数	相关参数（C，γ）	CPU 运行时间/s	错误分类	支持向量
3	3 568	Linear	DEFAULT	182.17	89	271
3	3 568	Linear	0.5,0.5	37.60	1 236	16
3	3 568	Linear	1.0,0.5	2.86	2 306	14
3	3 568	Linear	1.0,1.0	13.15	2 306	14
3	3 568	Linear	2.0,1.0	2.93	2 306	12
3	3 568	Radial	DEFAULT	2.29	54	935
3	3 568	Radial	0.5,0.5	1.79	51	810
3	3 568	Radial	1.0,0.5	2.14	37	796
3	3 568	Radial	1.0,1.0	3.38	39	923
3	3 568	Radial	2.0,1.0	2.75	36	902
3	3 568	Sigmoid	DEFAULT	1.48	1 235	2 396
3	3 568	Sigmoid	0.5,0.5	1.59	1 235	2 396
3	3 568	Sigmoid	1.0,0.5	1.33	1 235	2 396
3	3 568	Sigmoid	1.0,1.0	1.36	1 235	2 396
3	3 568	Sigmoid	2.0,1.0	1.48	1 235	2 396

表 5　　黑洞攻击测试数据集

输入特征参数个数	测试数据	核函数	正确个数	错误个数	IDS 准确性/%	Precision/ Recall
3	3 568	Linear	3 479	89	97.50	99.78%/96.25%
3	3 568	Linear	2 332	1 236	65.36	65.05%/99.91%
3	3 568	Linear	1 262	2 306	35.37	50%/0.09%
3	3 568	Linear	1 262	2 306	35.37	50%/0.09%
3	3 568	Linear	1 262	2 306	35.37	50%/0.09%
3	3 568	Radial	3 514	54	98.48	98.63%/98.97%
3	3 568	Radial	3 517	51	98.57	98.84%/98.92%
3	3 568	Radial	3 531	37	98.96	99.39%/98.92%
3	3 568	Radial	3 529	39	98.90	99.35%/98.92%
3	3 568	Radial	3 532	36	98.99	99.74%/99.0%
3	3 568	Sigmoid	2 333	1 235	65.39	65.05%/100%
3	3 568	Sigmoid	2 333	1 235	65.39	65.05%/100%
3	3 568	Sigmoid	2 333	1 235	65.39	65.05%/100%
3	3 568	Sigmoid	2 333	1 235	65.39	65.05%/100%
3	3 568	Sigmoid	2 333	1 235	65.39	65.05%/100%

的黑洞攻击的检测结果和已有模型检测结果做比较，具体的结果如表 6 所示[19,20]。

由此可以看出，本节设计的攻击检测方案能够有效地检测黑洞攻击。在第 3 节中提出的基于朋友机制的入侵检测模型中，可以将黑洞攻击生成的模型文件配置在入侵检测引擎模块，并且通过收集更多的网络审计数据不断的更新朋友关系列表，从而保持最新的直接朋友和间接朋友关系，使之相互协作、快速准确地对恶意节点行为做出判断，提升整个系统检测的准确性。

表 6　　黑洞攻击下的检测模型性能比较

序号	相关模型	检测率	误报率
1	1-SVMDM	85.58%	20.85%
2	2- SVMDM	96.95%	4.86%
3	SVM 模型	98.20%	0.30%
4	本文提出的模型	99.00%	0.26%

5 结束语

本文引入朋友机制的概念，提出了一种针对移动 ad hoc 网络的轻量级入侵检测模型，仿真实验证明，在检测路由中黑洞攻击时有着良好的性能，并在有限样本条件下，和已有入侵模型检测结果做了比较，检测准确率最高，进一步验证了本文所提模型的可行性和有效性。本文只针对网络路由层面的攻击进行了仿真实现。然而，要设计一个成熟的能够检测任何网络攻击的检测系统，不能只停留于网络路由层的攻击，需要扩展到链路层、传输层、甚至应用层去研究更新的安全威胁和攻击模型来丰富其规则库和网络轮廓，采取渐进的方式不断地对其完善。

参考文献：

[1] YANG C T, *et al*. A specification-based intrusion detection system for AODV[A]. Proc of the ACM Workshop on security of Ad Hoc and SensorNetworks[C]. 2003.125-134.

[2] HUANG Y, FAN W, LEE W, *et al*. Cross-featurea nalysisf or detecting ad-hoc routing anomalies[A]. Proceedings of the 23rd Intemational Conference On Distributed Computing Systems[C]. 2003. 478-487.

[3] SRINIVASARAO G, KUMAR S S. An Efficient Intrusion Detection System in Mobile Ad hoc Networks[A]. Lecture Notes in Electrical Engineering 151[C]. 2013.

[4] KULKARNI P. Design of hierarchical intrusion detection unit for ad hoc networks based on bayesian networks[M]. Dissertations & These grad works, 2008.

[5] PERRIG A, ZAPATA, JOHNSON D B. Ariadne: a secure on-demand routing protocol for ad hoc networks[A]. Mobile Computing and Networking ACM[C]. 2002. 12-23.

[6] JOHN C E Fast training of support vector machines using sequential minimal optimization[M]. Advances in Kernel Methods Support Vector Learning, Cambridge, MA, M/T Press, 1999: 185-208.

[7] KEERTHI S S, SHEVADE S K BHATTACHARYYA C, *et al*. Improvements to Platt's SM4 algorithm for SVM classifier design[D]. Dept. of O Mechanical and Production Engineering, National University of Singapore, 1999.

[8] JOACHIMS T. Making Large-Scale SVM Learning Practical[R]. LS8-Report, University of Dortmund, 1998.

[9] CHANG C C, LIN C J. LIBSVM: a library for support vector machines[EB/OL]. http:// www.csie.ntu.edu.tw/. rcjlinhibsvm, 2001.

[10] MILGRAM S. The small world problem[J]. Psychology Today, 1967, (5):60-67.

[11] HELMY A. Small worlds in wireless networks[J]. IEEE Communications Letters, 2003, 7(10): 490-492.

[12] CAPKUN S, HUBAUX J P, BUTTYAN L. Mobility helps security in ad hoc networks[A]. Proc of MobiHoc'03, Annapolis[C]. 2003. 45-56.

[13] PEI W D, CHEN Z Q, YUAN Z Z. Friends-help mechanism for generating a class of scale-free networks [J]. Journal of Jilin University (Information Science Edition) 2007, 25(4): 371-378.

[14] MA C E，SHI H S. Security model and mathematical analysis of mobile ad hoc network [J] . Chinese Journal of Sensors and Actuators, 2006, 19(4):1305-1309.

[15] RAGHAVAN B, SNOEREN A C. Priority forwarding in ad hoc networks with self-interested parties[A]. Workshop on Economics of Peer-to-Peer Systems[C]. Berkeley, USA, May, 2003.

[16] MIRANDA H, RODRIGUES L. Friends and foes: preventing selfishness in open mobile ad hoc networks[A]. Proc of the First International Workshop on Mobile Distributed Computing (MDC'03)[C]. USA, 2003.

[17] VAPNIK V N. The nature of statistical learning theory[A]. Series: Information Science and Statistics[C].1996.

[18] RAZAK S A, FURNELL S, CLARKE N, *et al*. A two-tier intrusion detection system for mobile ad hoc networks–a friend approach[A]. Intelligence and Security Informatics[C]. Springer Berlin Heidelberg, 2006. 590-595.

[19] DENG H M, ZENG Q A, AGRAWAL D P. SVM-based intrusion detection system for wireless ad hoc networks[A]. Vehicular Technology Conference[C]. 2003.

[20] WANG X; WONG J S, STANLEY F, BASU S. Cross-layer based anomaly detection in wireless mesh networks[A]. Ninth Annual International Symposium on Applications and the Internet[C]. 2009. 20-24.

作者简介：

肖阳（1991-），男，新疆石河子人，西安电子科技大学博士生，主要方向为信任管理、可信计算。

白磊（1993-），男，河南漯河人，西安电子科技大学硕士生，主要研究方向为网络与信息安全、无线传感器网络。

王仙（1987-），女，陕西富平人，西安电子科技大学硕士生，主要研究方向为网络安全防御及检测、网络攻防等。