基于图论的 MANET 入侵检测方法

张冰涛*①② 王小鹏① 王履程① 张忠林① 李延林③ 刘 虎①
①(兰州交通大学电子与信息工程学院 兰州 730070)
②(兰州大学信息科学与工程学院 兰州 730000)
③(中国科学院近代物理研究所 兰州 730000)

摘 要：移动 Ad hoc 网络(MANET)易遭受各种安全威胁，入侵检测是其安全运行的有效保障，已有方法主要关注特征选择以及特征权重，而忽略特征间潜在关联性，针对此问题该文提出基于图论的 MANET 入侵检测方法。首先通过对典型攻击行为分析，合理选择 9 种特征作为节点，依据欧式距离确定节点间的边以构建结构图。其次发掘节点(即特征)间关联性，综合考虑节点邻居规模属性和节点邻居之间的紧密程度属性，利用图论所对应的统计特性度分布和聚集系数具体实现两属性。最后对比实验结果证明此方法与传统方法相比平均检测率和误检率分别提高 10.15%、降低 1.8%。

关键词：入侵检测；移动 Ad hoc 网络；图论；特征关联性
中图分类号：TP393.06 **文献标识码**：A **文章编号**：1009-5896(2018)06-1446-07
DOI: 10.11999/JEIT170756

Intrusion Detection Method for MANET Based on Graph Theory

ZHANG Bingtao①② WANG Xiaopeng① WANG Lücheng①
ZHANG Zhonglin① LI Yanlin③ LIU Hu①
①(*School of Electronic and Information Engineering*, *Lanzhou Jiaotong University*, *Lanzhou* 730070 *China*)
②(*School of Information Science and Engineering*, *Lanzhou University*, *Lanzhou* 730000 *China*)
③(*Institute of Modern Physics*, *Chinese Academy of Sciences*, *Lanzhou* 730000 *China*)

Abstract: Mobile Ad hoc NETwork (MANET) is vulnerable to various security threats, and intrusion detection is an effective guarantee for its safe operation. However, existing methods mainly focus on feature selection and feature weighting, and ignore the potential association among features. To solve this problem, an intrusion detection method for MANET based on graph theory is proposed. First of all, nine features are selected as nodes based on the analysis of typical attack behavior, and the edges among nodes are determined according to Euclidean distance so as to build the structure diagram. Secondly, the scale attributes of neighborhood nodes and the degree of closeness attributes among nodes are considered to explore (i.e. feature) the correlation among nodes, then the statistical properties degree distribution and clustering coefficient of graph theory are used to realize the above two attributes. Finally, contrasting experimental results show that compared with the traditional methods, the average detection rate and false detection rate of new method are improved by 10.15% and reduced by 1.8% respectively.

Key words: Intrusion detection; Mobile Ad hoc NETwork (MANET); Graph theory; Feature correlation

1 引言

移动Ad hoc网络[1–3]无固定基础设施，网络节点既是主机又是路由器，具有较强的自组织能力和实时部署能力。同时，MANET无线信道的开放性使得网络节点以不可预知方式不断加入或者离开网络，导致信息交互过程中易遭受到各种攻击，如泛洪攻击、伪造攻击、丢包攻击、黑洞攻击等。因此及时有效检测出各种入侵行为是MANET安全保护的重要屏障。

依据入侵检测所采用技术，通常入侵检测[4]分为：误用检测和异常检测。误用检测通过对已知攻

收稿日期：2017-07-25；改回日期：2018-02-28；网络出版：2018-04-02
*通信作者：张冰涛 zhangbingtao321@163.com
基金项目：国家自然科学基金(61761027, 61261029, 61662043)，兰州交通大学青年基金(2016004)
Foundation Items: The National Natural Science Foundation of China (61761027, 61261029, 61662043), The Yong Scholar Fund of Lanzhou Jiaotong University (2016004)

击特点分析，确认恶意攻击；异常检测通过对正常行为分析去识别不合理的网络访问，确认恶意攻击。此外，异常检测也能够有效地检测未知入侵。本文研究基于后者思想，通过对正常网络属性分析，确定9种攻击特征，进而实现入侵检测。

当前异常入侵检测方法侧重于特征选择以及特征权重。文献[5]采用包装器特征选择算法计算所有节点特征权重，根据设定门限值识别最优特征子集，基于决策树分类器完成异常入侵检测。Fidalcastro等人[6]指出对于MANET使用经典序列模式挖掘算法从海量多维网络信息中识别正常行为和异常行为虽表现良好，但是生成候选特征过程缓慢。因此，提出基于混合逻辑特征选择和混合权重支持的半监督式序列模式挖掘算法，依据特征权重优先级，并省略优先级较低候选特征的计算，从而提高算法执行效率。文献[7]提出基于改进K-means算法的MANET异常检测方法，引入划分贡献度概念，计算各维度的特征在入侵检测中所占权重，将遗传算法与K-means算法结合实现异常入侵检测，此外，利用MapReduce计算框架提高检测效率，解决海量数据异常检测问题。文献[8]提出一种新的混合网络入侵检测系统，使用智能动态群粗糙集进行特征选择，加权局部搜索策略与简化群优化分类器结合实现异常入侵检测，分类准确率达到93.3%。尽管上述方法具有各自不同优势，对入侵检测技术发展起到推动作用，但是均未考虑特征节点之间的关联性。

图论广泛运用于与复杂网络有关的领域，Li等人[9]将图论作为工具识别正常和异常脑功能区域，使用先进医学技术标记正常和异常脑功能关注区域(ROI)，基于关注区域的扩散张量成像建立脑结构网络，依据图论基础计算脑结构网络的全局和局部属性并作为特征完成正常和异常脑功能区域划分。Zhu等人[10]基于图论将脑电(EEG)信号映射至可视图和水平可视图，然后提取典型的图特征，并转发到支持向量机(SVM)分类器完成睡眠分期任务。Zhang等人[11]以图论为基础，建立静息状态脑功能网络，帮助外科医生诊断轻度认知损伤(MCI)，以达到延迟和阻止阿兹海默症(AD)的目的。近来，文献[12]提出基于图论的入侵检测方法，首次将图论的思想引入入侵检测，其核心思想为：将数据对象之间相似度关系转换至图的邻接矩阵，再将邻接矩阵转换为关联矩阵，以表示数据对象之间的相似关系；然后利用最速下降法求得最佳转换矩阵，以完成关联矩阵的块对角矩阵转换而达到数据聚类效果，从而识别正常数据与入侵数据。

本文受到上述图论应用思想启发，从传统MANET 入侵检测对特征间潜在关联性考虑不足出发，提出基于图论的 MANET 入侵检测方法， 其主要工作在于：(1)以详细分析 MANET 易遭受泛洪攻击、伪造攻击、丢包攻击、黑洞攻击等典型攻击为基础，选择最有效特征属性以表示攻击特性；(2)以特征属性为节点，节点间欧式距离为边建立结构图；(3)使用度分布和聚集系数等统计属性完成对节点间关联性的承载，利用 K-means 分类器实现MANET 入侵检测。

2　入侵检测模型

为说明入侵检测方法的有效性，将 MANET 入侵检测问题转化为对典型攻击行为的识别。图 1 给出基于图论的 MANET 入侵检测方法模型框图，主要包含 4 个部分：(1)原始 MANET 数据；(2)攻击特征选取；(3)核心检测模块，其中结构图构建过程中借鉴了文献[12]的部分思想，即欧式距离度量指标，文献[12]利用欧式距离度量数据对象之间的相似度，本文研究借鉴于此采用欧式距离(和门限值 δ)确定图中顶点之间是否连通；(4)入侵检测结果。此外，还将新提出方法与传统方法进行对比。本文研究重点是攻击特征选取及核心检测模块，因此对其它部分只作简单介绍。

2.1 攻击特征的选取及标准

从原始 MANET 数据中可提取多种用于攻击检测的特征属性[13]，本文研究仅选取其中 9 种，如表 1

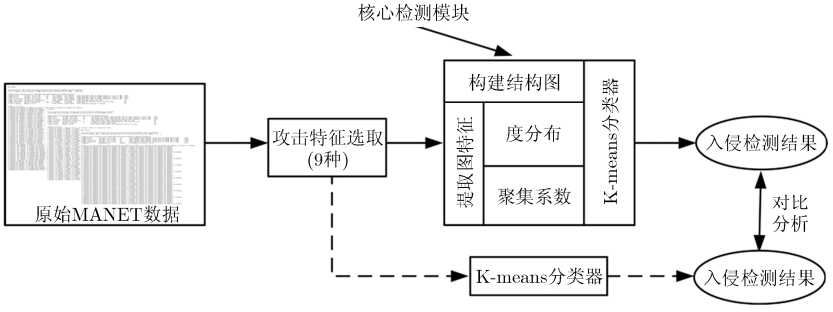

图 1 基于图论的 MANET 入侵检测方法模型

所示，其主要动机和标准可归纳为：

(1)仿真环境下，恶意节点发送大量路由请求(RREQ)模拟泛洪攻击。此情形下，恶意节点特征 2, 5 急剧增加，正常节点特征 3, 4 明显增加，特征 9 可能增加。

(2)仿真环境下，恶意节点定向发送路由错误(RERR)至正常节点，导致重复链路故障模拟伪造攻击。此情形下，恶意节点及选定正常节点特征 6, 7 分别明显增加。

(3)仿真环境下，恶意节点丢弃全部 RERR，导致正常节点向断开路径转发数据包以模拟丢包攻击。此情形下，特征 6, 7 急剧减少，特征 8 显著增加。

(4)仿真环境下，恶意节点对接收到的全部 RREQ 做出及时路由请求(RREP)响应，声明自己具有最小路径，骗取正常节点与其建立路由链接，然后实施恶意操作(如丢弃接收到的数据包)以模拟黑洞攻击。此情形下，恶意节点特征 1, 4 急剧增加。

表 1 9 种攻击特征

编号	特征名	含义或计算方法
1	Data received	节点接收数据包的数目
2	RREQ sent	节点发送 RREQ 的数目
3	RREQ received	节点接收 RREQ 的数目
4	RREP sent	节点发送 RREP 的数目
5	RREP received	节点接收 RREP 的数目
6	RERR sent	节点发送 RERR 的数目
7	RERR received	节点接收 RERR 的数目
8	Broken Links	$\mathrm{BL}=\sum_{\text{nodes}}\text{linkfailure}$
9	Packets Dropped Rate	$\mathrm{PDR}=\dfrac{\text{Packetsdropped}}{\text{Packetsoriginated}}$

2.2 基于图论的核心检测模块

核心检查模块基本思想概括为：权衡获取信息量与算法运行时间，每 15 s 作为一个时间窗口(采样间隔)提取一组特征。如图 2 所示，每组特征构成一个特征向量，计算特征向量中所有特征间欧几里德距离。依据欧式距离构建特征点结构图，确定对应的邻接矩阵，从矩阵中获取图论所对应的两类统计属性，进而通过 K-means 分类器检测异常攻击行为。

2.2.1 图及其邻接矩阵的构建 以特征向量中的特征点作为结构图 $G=(V,E)$ 的节点，9 个特征点即 $V=9$。由图论知识[14]可知假设图中有 V 个顶点，E 条边，则含有 $E=V(V-1)/2$ 条边的无向图称作完全图。因此，本文研究中 E 的最大取值为 36，即 $E\le 36$。

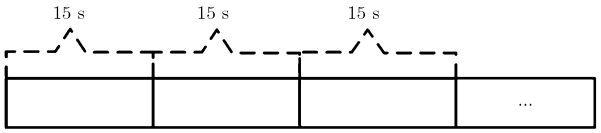

图 2 特征提取周期

每个攻击特征是一个现实空间的时间序列数据集合，通常计算特征间的相关性(或相似性)有两种度量方法[12,15]：距离度量和相关系数度量。本文采用前者，利用欧氏距离度量特征之间的相关性。首先将现实空间时间序列数据转化至几何空间，然后再通过计算几何空间中的欧式距离来反映不同特征间的相关性程度。

n 维欧式空间是一个点集，每一个点 $\boldsymbol{X}$ 可以表示成一个向量 $(x[1],x[2],\cdots,x[n])$。因为本研究中每个特征点是一个时间序列集合，所以结构图中节点之间的欧式距离可以表示为

$$d(\boldsymbol{A},\boldsymbol{B})=\sqrt{\sum_{i=1}^{n}\big(a[i]-b[i]\big)^2} \tag{1}$$

其中，$d(\boldsymbol{A},\boldsymbol{B})$ 表示图中任意两点 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 之间的欧式距离，节点 $\boldsymbol{A}$,$\boldsymbol{B}$ 可以分别表示为 $\boldsymbol{A}=(a[1],a[2],\cdots,a[n])$ 和 $\boldsymbol{B}=(b[1],b[2],\cdots,b[n])$。节点间连通性由其欧式距离与自适应门限值 δ 确定，若 $d(\boldsymbol{A},\boldsymbol{B})\le\delta$，则节点 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 连通，否则不连通。

每组特征向量门限值 δ 由节点间的连通率自适应确定，不同的实验环境 δ 不同。本文研究中 δ 基于 3.1 节仿真实验环境及表 2 的算法确定。

表 2 寻找最佳门限 δ

算法：寻找最佳门限 δ

输入：(a) $E=36$; %连通的边数目上限

(b) $p=0$, $\delta_{\text{best}}=0$, $\text{TPR}_{\text{best}}=0$; %最优连通率，最佳门限，最优检测率的初始化

(1) for $i=[0.05:0.05:1]$

(2) $\delta=E*i$;

(3) 依据门限值 δ 和节点间的欧式距离生成结构图，以及邻接矩阵；

(4) 提取图特征：度分布，聚集系数；

(5) 转发图特征至 K-means 分类器，获得 TPR 和 FPR；

(6) if $\text{TPR}_{\text{best}}\le\text{TPR}$

(7) TPR_{best}=TPR, $p=i,\delta_{\text{best}}=\delta$;

(8) end

(9) end

输出：p , δ_{best}。

此研究中两个最优连通率(基本相等)出现在 0.25 与 0.30，即 25% ($E=9$)至 30% ($E=10$)。最终选取了门限值 $\delta=10$ 。

图 3 给出一组特征向量生成的结构图 G ，以及相应欧式距离。文献[12]提出将入侵数据之间的相似特征关系转换至邻居矩阵，然后，通过进一步转换处理，最终得到块对角矩阵用于区分正常数据与异常数据。其中邻接矩阵反映不同入侵数据之间的相似特征，受此思想启发，本文首先将图存储于邻居矩阵，然后再利用邻接矩阵发掘入侵数据之间的潜在关联性。表 3 给出了图 3 所对应的邻接矩阵，图的统计属性计算(见 2.2.2 节)仅与节点之间连通性有关，与权值无关，依据邻接矩阵节点间的连通性可以改写为

$$d(\boldsymbol{A},\boldsymbol{B})=\begin{cases}1, & (\boldsymbol{A},\boldsymbol{B})\in E\\ 0, & \text{其它}\end{cases} \tag{2}$$

2.2.2 图的统计属性　图邻接矩阵的统计属性蕴含着节点之间潜在关联性，因此本文使用度分布和聚集系数等统计属性检测异常攻击行为。

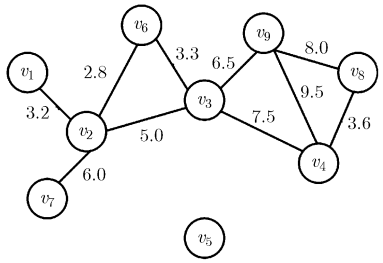

图 3 特征向量的生成结构图

表 3 图 G 所对应的邻接矩阵

	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9
v_1	0	1	0	0	0	0	0	0	0
v_2	1	0	1	0	0	1	1	0	0
v_3	0	1	0	1	0	1	0	0	1
v_4	0	0	1	0	0	0	0	1	1
v_5	0	0	0	0	0	0	0	0	0
v_6	0	1	1	0	0	0	0	0	0
v_7	0	1	0	0	0	0	0	0	0
v_8	0	0	0	1	0	0	0	0	1
v_9	0	0	1	1	0	0	0	1	0

(1)度分布：　度分布[16]是指图中节点度数的概率分布，体现了各个节点度的散布程度。本文用其描述节点的邻居规模。$P(k)$ 表示图中度数为 k 的节点的度分布，计算过程如式(3)：

$$P(k)=\frac{\left|\{v\mid d(v)=k\}\right|}{N} \tag{3}$$

其中， $d(v)$ 表示节点 v 的度， N 表示图中节点的总数。间隔 15 s 获取一组度分布特征，由 $V=9$ 可知节点度分布特征数取值范围为 1~8。表 4 给出表 3 中 G 图所对应邻接矩阵的度分布，其包含度分布特征数为 5。

表 4 图 G 对应的度分布

k	0	1	2	3	4
$P(k)$	1/9	2/9	2/9	2/9	2/9

(2)聚集系数：　聚集系数[17]是指图中节点的聚集程度，常用于描述图的局部结构或者全局结构的连接紧密程度。体现了节点的邻接节点互为邻接的比例，表示为

$$C v_i=\frac{2e_i}{d(v_i)\big(d(v_i)-1\big)} \tag{4}$$

其中， e_i 表示节点 v_i 与任意两邻接节点形成三角形的个数，$d(v_i)$ 表示节点 v_i 的度。表 5 给出表 3 中 G 图所对应邻接矩阵中各节点的聚集系数。

整个图的聚集系数是图中所有节点聚集系数的均值，本文用其描述节点邻居之间的紧密程度，以检测异常攻击行为，计算过程如式(5)：

$$C=\frac{1}{N}\sum_{i=1}^{N}Cv_i \tag{5}$$

其中， N 表示图中节点数量，由式(5)可知表 3 中图 G 的聚集系数为 0.43。

2.2.3 入侵检测及性能评估　构建 15 s 时间窗口的结构图，计算度分布和聚集系数等统计属性存放于 2 维表，表中每条记录由两部分组成：特征属性和类属性。度分布的本质决定了不同结构图对应特征属性数量是随机数，取值范围为 1~9(度分布属性取值 1~8，聚集系数属性取值 1)。类属性为特征属性对应的实际网络状态：正常或者异常(泛洪攻击、伪

表 5 图 G 对应的聚集系数

节点 v_i	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9
度 $d(v_i)$	1	4	4	3	0	2	1	2	3
局部聚集系数 Cv_i	0	0.17	0.33	0.67	0	1.00	0	1.00	0.67

造攻击、丢包攻击、黑洞攻击)。表中每条记录作为K-means 分类器的一个输入用于评估入侵检测性能。此外，为获得统计学意义上的结果，K-means分类器执行 10 次 10 折交叉验证，也就是迭代执行10 次，意味着 100 次调用分类器。

为有效评估入侵检测性能，采用衡量入侵检测结果准确性指标[18]：检测率(TPR)和误检率(FPR)，其分别定义为

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{6}$$

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{TN}+\mathrm{FP}} \tag{7}$$

TP表示将异常攻击行为检测为异常攻击行为的数量，FP表示将异常攻击行为检测为正常行为的数量，FN表示将正常行为检测为异常攻击行为的数量，TN表示将正常行为检测为正常行为的数量。最后以10次10折交叉验证算术平均检测率和误检率作为入侵检测结果。

3 实验仿真与结果

为验证入侵检测模型的有效性，进行两组实验的对比。第 1 组试验从原始数据记录中选取 9 种攻击特征作为 K-means 分类器的输入直接进行入侵检测。第 2 组试验使用 9 种攻击特征构建结构图，计算图对应的邻接矩阵，从矩阵中提取图的特征属性度分布和聚集系数作为 K-means 分类器输入进行入侵检测。

3.1 仿真环境

仿真实验使用 NS2 软件模拟一个 1000 m×1000 m 的 MANET 网络环境，50 个移动节点分布其中。节点的无线传输范围(Radio propagation range)为 250 m，信道容量(Channel capacity)为 2 Mbit/s。路由协议为 AODV，采用“Random way point”节点模型移动，最小、最大移动速度分别设置为 0 和 30 m/s。节点产生并发送固定比特率(Constant bit rate)数据包，包尺寸从 128 Byte 到 1024 Byte 不等。仿真环境下，节点从静止开始随机选择一个目的位置，移动到达目的位置，停留等待一个设定时间后，继续随机选择并移动，重复此过程直到实验结束，每次实验仿真时长为 900 s。详细仿真参数设置见表 6。

通过修改停留等待时间(0 s, 300 s, 600 s 和 900 s)，节点最大移动速度(10 m/s, 20 m/s 和 30 m/s)，攻击节点比例(10%, 30%和 50%)等参数，仿真实验共进行 36 次模拟，获得时长 32400 s 原始数据。采样间隔与图 2 特征提取周期相同，即 15 s，每次采样后标记统计数据类型为：正常、泛洪攻击、伪造攻击、丢包攻击、黑洞攻击。最后，把所有标记数据随机混合得到 2160 条原始数据，详细记录见表 7。

表 6 参数设置

参数名	参数值
协议类型	AODV
仿真时长(s)	900
仿真区域(m^2)	1000×1000
节点数量	50
节点移动模型	随机路径模型
信道容量(Mbit/s)	2
节点无线传输范围(m)	250
最小移动速度(m/s)	0
最大移动速度(m/s)	30
攻击节点比例(%)	10, 30 和 50
等待时间(s)	0, 300, 600 和 900
采样周期(s)	15

改进网络代理监测部署算法[19](IDANMA)的独立决策机制被用于本实验中入侵检测算法的部署。基于文献[19]实验结果：两轮投票选举策略在规定通信半径内可达节点最多的节点为决策代理和网络监测代理节点。本实验将入侵检测算法(决策代理)与各节点信息收集(网络数据包监测)部署在同一节点上。虽然此方案在一定程度上增加了被部署节点的能量消耗，但不会影响算法的检测效率。

表 7 原始数据

数据类型	数量(条)
正常	1512
泛洪攻击	162
伪造攻击	162
丢包攻击	162
黑洞攻击	162

MATLAB 软件(版本：R2012b)用于提取原始记录中 9 种攻击特征，生成结构图的邻居矩阵以及提取图的统计特征属性度分布和聚集系数。WEKA 软件(版本：3.7.11)用于实现异常攻击行为检测。

3.2 实验结果

图 4，图 5 分别给出两组实验(基于图论的 MANET 入侵检测和直接使用 K-means 分类器的 MANET 入侵检测)检测率和误检率的结果。由图 4 可知，基于图论的入侵检测率明显高于直接使用原始记录中 9 种攻击特征作为 K-means 分类器输入的检测率，这可能是因为图的统计特征发掘出零散攻

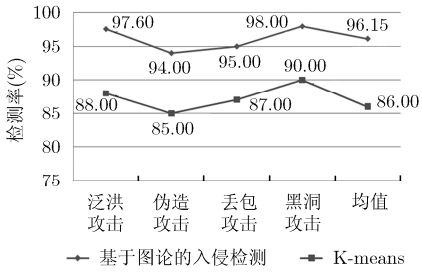

图 4　4 种典型攻击的检测率及其平均值

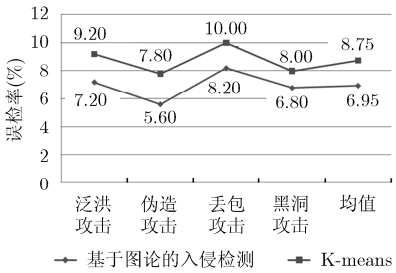

图 5　4 种典型攻击的误检率及其平均值

击信息之间内在联系，从而获得更高检测率。同时，如图 5 所示降低了误检率。

若不考虑泛洪攻击、伪造攻击、丢包攻击、黑洞攻击之间的差异性，将 4 种攻击均作为异常行为处理，异常入侵检测就可描述为正常行为和异常行为的 2 类问题检测。真实环境下，可能重点考虑的是攻击是否发生，而对具体何种攻击并不关心。因此，本文也对比了 5 类问题(正常、泛洪攻击、伪造攻击、丢包攻击、黑洞攻击)检测与 2 类问题(正常行为、异常行为)检测。表 8 给出两组实验下(基于图论的MANET入侵检测和直接使用K-means分类器的MANET入侵检测)5类问题检测和2类问题检测的平均检测率。从表 8 可知，2 类问题平均检测率明显高于 5 类问题检测率，也就是说真实环境下，当不考虑具体攻击时，基于图论的 MANET 入侵检测方法检测率还将提高 1.85%。

表 8　5 类问题与 2 类问题的平均检测率对比(%)

	基于图论的入侵检测	K-means
5 类	96.15	86.00
2 类	98.00	89.00

4　结束语

本文提出基于图论的 MANET 入侵检测方法，将图论知识运用到入侵检测中，挖掘攻击特征之间内在关联性，取得了较好的实验效果。首先，研究分析了泛洪攻击、伪造攻击、丢包攻击、黑洞攻击等 4 种常见 MANET 攻击行为，使用攻击特征建立图论所对应的结构图以及邻接矩阵，通过度分布和聚集系数发掘潜在节点邻居规模属性和节点邻居之间的紧密程度属性实现异常入侵检测。最后，对比实验结果表明本文所提出的 MANET 入侵检测方法相比传统方法具有较高的检测率，较低误检率。此外，仅考虑异常和正常两类检测问题时检测率还会提高 1.85%。

参 考 文 献

[1] 冯涛, 郭显, 马建峰, 等. 可证明安全的节点不相交多路径源路由协议[J]. 软件学报, 2010, 21(7): 1717–1731. doi: 10.3724/SP.J.1001.2010.03576.
FENG Tao, GUO Xian, MA Jianfeng, *et al*. Provably secure approach for multiple node-disjoint paths source routing protocol[J]. *Journal of Software*, 2010, 21(7): 1717–1731. doi: 10.3724/SP.J.1001.2010.03576.

[2] VADIVEL R and BHASKARAN V M. Adaptive reliable and congestion control routing protocol for MANET[J]. *Wireless Networks*, 2016, 23(3): 819–829. doi: 10.1007/s11276-015-1137-3.

[3] SINGAL G, LAXMI V, GAUR M S, *et al*. Multi-constraints link stable multicast routing protocol in MANETs[J]. *Ad Hoc Networks*, 2017, 63: 115–128. doi: 10.1016/j.adhoc.2017.05.007.

[4] INDIRANI G and SELVAKUMAR K. A swarm-based efficient distributed intrusion detection system for mobile Ad hoc networks (MANET)[J]. *International Journal of Parallel, Emergent and Distributed Systems*, 2014, 29(1): 90–103. doi: 10.1080/17445760. 2013.773001.

[5] SINDHU S S S, GEETHA S, and KANNAN A. Decision tree based light weight intrusion detection using a wrapper approach[J]. *Expert Systems with Applications*, 2012, 39(1): 129–141. doi: 10.1016/j.eswa.2011.06.013.

[6] FIDALCASTRO A and BABURAJ E. Sequential pattern mining for intrusion detection system with feature selection for MANETS[J]. *Asian Journal of Research in Social Sciences and Humanities*, 2017, 7(2): 428–442. doi: 10.5958/2249-7315. 2017.00100.9.

[7] 李洪成, 吴晓平, 严博. 面向MANET异常检测的分布式遗传k-means 研究[J]. 通信学报, 2015, 36(11): 167–173. doi: 10.11959/j.issn.1000-436x.2015269.
LI Hongcheng, WU Xiaoping, and YAN Bo. Research on distributed genetic k-means for anomaly detection in MANET[J]. *Journal on Communications*, 2015, 36(11): 167–173. doi: 10.11959/j.issn.1000-436x.2015269.

[8] CHUNG Y Y and WAHID N. A hybrid network intrusion detection system using simplified swarm optimization

(SSO)[J]. *Applied Soft Computing*, 2012, 12(9): 3014–3022. doi: 10.1016/j.asoc.2012.04.020.

[9] LI Xiaojin, HU Xintao, JIN Changfeng, *et al*. A comparative study of theoretical graph models for characterizing structural networks of human brain[J]. *International Journal of Biomedical Imaging*, 2013, 13(1): 27–35. doi: 10.1155/2013/201735.

[10] ZHU Guohun, LI Yan, and WEN P P. Analysis and classification of sleep stages based on difference visibility graphs from a single-channel EEG signal[J]. *IEEE Journal of Biomedical & Health Informatics*, 2014, 18(6): 1813–1821. doi: 10.1109/JBHI.2014.2303991.

[11] ZHANG Xiaowei, HU Bin, MA Xu, *et al*. Ontology driven decision support for the diagnosis of mild cognitive impairment[J]. *Computer Methods and Programs in Biomedicine*, 2014, 113(3): 781–791. doi: 10.1016/j.cmpb.2013.12.023.

[12] 包振, 何迪. 一种基于图论的入侵检测方法[J]. 上海交通大学学报, 2010, 44(9): 1176–1180.
BAO Zhen and HE Di. An intrusion detection method based on graph theory[J]. *Journal of Shanghai Jiaotong University*, 2010, 44(9): 1176–1180.

[13] MITROKOTSA A and DIMITRAKAKIS C. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection[J]. *Ad Hoc Networks*, 2013, 11(1): 226–237. doi: 10.1016/j.adhoc.2012.05.006.

[14] 严蔚敏, 陈文博. 数据结构及应用算法教程(修订版)[M]. 北京: 清华大学出版社, 2011: 201–202.
YAN Weimin and CHEN Wenbo. Data Structure and Application Algorithm Tutorial(Revised Edition)[M]. Beijing: Tsinghua University Press, 2011: 201–202.

[15] TAKIGUCHI J, LWAMA K, KOZAKI M, *et al*. A study of autonomous mobile system in outdoor environment[J]. *IFAC Computer Aided Control Systems*, 1997, 30(4): 61–66. doi: 10.1016/S1474-6670(17)43613-5.

[16] 王林, 戴冠中. 复杂网络的度分布研究[J]. 西北工业大学学报, 2006, 24(4): 405–409.
WANG Lin and DAI Guanzhong. On degree distribution of complex network[J]. *Journal of Northwestern Polytechnical University*, 2006, 24(4): 405–409.

[17] 任卓明, 邵凤, 刘建国, 等. 基于度与集聚系数的网络节点重要性度量方法研究[J]. 物理学报, 2013, 62(12): 522–526. doi: 10.7498/aps.62.128901.
REN Zhuoming, SHAO Feng, LIU Jianguo, *et al*. Node importance measurement based on the degree and clustering coefficient information[J]. *Acta Physica Sinica*, 2013, 62(12): 522–526. doi: 10.7498/aps.62.128901.

[18] ZHANG Xiaowei, HU Bin, MA Xu, *et al*. Resting-State whole-brain functional connectivity networks for MCI classification using L2-Regularized logistic regression[J]. *IEEE Transactions on Nanobioscience*, 2015, 14(2): 237–247. doi: 10.1109/TNB.2015.2403274.

[19] 李玲娟, 徐向凯, 王汝传. MANET 的 IDS 中移动代理部署算法的研究[J]. 南京邮电大学学报(自然科学版), 2006, 26(3): 52–57.
LI Lingjuan, XU Xiangkai, and WANG Ruchuan. Research of the mobile agent disposal algorithm in MANET IDS[J]. *Journal of Nanjing University of Posts and Telecommunications* (*Natural Science*), 2006, 26(3): 52–57.

张冰涛： 男，1986 年生，讲师，博士生，研究方向为网络安全、无线传感器网络.

王小鹏： 男，1969 年生，教授，博士生导师，主要研究方向为计算机图像图形处理、数字信号处理及应用、计算机视觉.

王履程： 男，1978 年生，讲师，博士生，研究方向为密码编码理论.

张忠林： 男，1965 年生，教授，主要研究方向为智能信息处理.

李延林： 男，1982 年生，工程师，主要研究方向为 Ad hoc 网络、网络安全.

刘 虎： 男，1983 年生，讲师，博士生，研究方向为密码编码理论、内容安全.