一种基于机器学习的MANET网络入侵检测性能评估方法研究

蒋一波 王雨晨 王万良 张 祯 陈 琼
(浙江工业大学计算机学院 杭州 310023)

摘 要 移动Ad hoc网络(MANET,Mobile Ad hoc Networks)正得到越来越广泛的应用,相应的网络安全问题也开始得到广泛的关注。研究MANET网络可能遭遇的攻击方式,提出基于机器学习技术的入侵检测性能评估模型,并提出一个综合评价指标,比较了7种机器学习算法在MANET网络入侵检测中的性能表现,对于构建安全有效的MANET网络具有重要的意义。使用GloMoSim仿真工具对MANET网络正常行为及黑洞、洪水、丢包3种入侵行为进行模拟,并详细分析了各种攻击情况下,7种机器学习算法的性能表现。分析结果显示,该评估模型能较好地反映出各种机器学习算法的性能,其中,多层感知器、逻辑回归和支持向量机具有较高的检测率及较低的误报率。

关键词 MANET,入侵检测,机器学习,性能评估
中图法分类号 TP393 **文献标识码** A

Performance Analysis Method for Intrusion Detection in MANETs Based on Machine Learning Algorithms

JIANG Yi-bo WANG Yu-chen WANG Wan-liang ZHANG Zhen CHEN Qiong
(College of Computer Science, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract Mobile Ad-hoc network (MANET) has become an important technology in recent years and the corresponding security problems is getting more and more attention. This paper proposed a performance analysis model and an integrated evaluation index for intrusion detection based on machine learning algorithms. The experiment simulated three typical anomalous behaviors (Black hole, Flooding and Packet drop) and compared seven well-known machine learning algorithms in detail. The analysis results show that the proposed model could give a well expression to the performance of each algorithm. In particular, MultiLayer Perceptron, Logistic Regression and Support Vector Machine give the best performance and the Logistic Regression and Support Vector Machine also spend very little time to train the classification model.

Keywords MANET, Intrusion detection, Machine learning algorithms, Performance analysis

1 引言

MANET由一些具有通信能力的移动设备组成,具有动态网络拓扑结构和自组织能力,并且在许多领域都有广泛应用。相比有线网络而言,MANET更容易受到入侵者的攻击。MANET使用无线信道进行通信,在无线信号范围内,攻击者可以很容易实现窃听并发起攻击[1-3]。当前,已经有许多方法被提出以检测网络中的异常活动行为,但研究大多关注单个算法的创新与改进(基于神经网络[9]、聚类[10]和支持向量机[12]等),缺乏在一个统一的数据集上对不同检测算法进行比较的研究。

本文针对MANET网络中3种入侵行为,提出了一种基于机器学习技术的入侵检测性能评估模型,建立了刻画网络流量的特征模型,提出了一个综合评价指标,综合考虑了检测率、误报率、训练时间和检测时间,并在此基础上比较了7种著名机器学习算法的性能表现。使用仿真工具对网络流量数据进行仿真、采样和统计处理,生成一系列数据集以对现实情况进行有效模拟。异常的网络节点在网络运行时发动各种攻击,这些攻击行为会以统计数据的形式被记录,并用于机器学习算法。

本文第2节对MANET及其安全问题进行简要介绍;第3节阐述了相关工作;第4节对7种机器学习算法以及提出的评估模型、评价指标等进行介绍;第5节展示了实验环境和性能分析结果;最后对本文进行总结。

2 MANET及其安全问题

2.1 MANET

移动Ad hoc网络诞生于1960年末和1970年初。1973年,美国国防部高级研究计划局DARPA资助了一项研究计划,Packet Radio Network(PRNET)[4],该网络是一种可以通过无线信道传输数据的包交换计算机通讯网。这些工作为MANET创造了先驱理论和实践。

本文受"十二五"国家科技支撑计划:农村小水电高效发电技术(2012BAD10B01)资助。
蒋一波(1982—),男,博士,副教授,主要研究方向为人工智能,E-mail:jyb106@zjut.edu.cn;王雨晨(1988—),男,硕士生,主要研究方向为人工智能;王万良(1957—),男,博士,教授,博士生导师,主要研究方向为计算机控制与智能自动化、人工智能及其应用;张 祯(1992—),男,主要研究方向为机器学习;陈 琼(1990—),女,硕士生,主要研究方向为人工智能。

MANET 不同于传统的有线网络。在 MANET 中，每一个节点都作为一个路由器为其他节点传输数据。通过互相的通信协作，这些移动节点共同为网络的正常运转负责。

2.2 MANET 网络安全

MANET 是一种特殊的无线网络。从网络结构角度看，该网络的主要特点是没有中心接入点，每一个网络节点都参与数据路由工作。任何一个节点发起异常攻击，都可能给整个网络带来巨大影响。此外，MANET 是一个开放网络，攻击者有更多机会入侵网络并发动各种攻击，例如，洪水(Flooding)、黑洞(Black Hole)和拒绝服务(DoS)等[5]。图 1 展示了一种含有攻击节点的 MANET 网络。

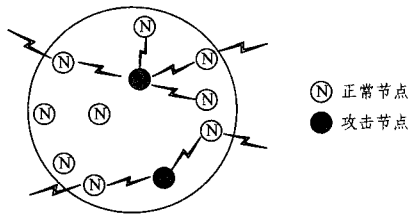

图 1 含有攻击节点的 MANET 网络示意图

我们通过模拟 3 种攻击来评估不同类型的机器学习算法：

(1)洪水攻击：攻击者广播大量伪造数据包，耗尽网络带宽资源，让网络无法正常工作。本实验模拟的异常节点向整个网络发出大量路由请求(RREQ)数据包，以达到消耗网络资源的目的。

(2)丢包攻击：该攻击中，异常节点丢弃发给它的数据包。本实验模拟的异常节点丢弃路由回复(RREP)包和数据信息包(Data)。

(3)黑洞攻击：异常节点向其他节点声明自己具有最小路由路径，骗取其他节点同其建立路由连接，然后进行异常行为。本实验模拟异常节点吸收其他节点发出的数据信息包(Data)，并丢弃。

3 相关工作

入侵检测已有 30 多年的发展历史，其概念最早由 Anderson[6]在 1980 年提出，他指出审计数据中包含十分有价值的数据，可以用于检测异常用户行为。随后，Denning[7]领导了斯坦福研究院对于入侵检测的相关工作，并提出了第一个入侵检测系统模型。

目前，有许多种实现入侵检测系统的方法，例如，基于统计、模式、规则以及状态的入侵检测系统。本文着重于使用有监督的机器学习算法，并在相同数据集上对不同算法的入侵检测性能进行评估。

Zhang 等[8]首先提出了 MANET 网络中的入侵检测模型，该系统十分类似于传统有线网络下的多 Agent 入侵检测系统。每一个节点既可以监控自己的活动情况也可以监控其邻居节点行为。这些工作为后续在 MANET 中建立一个高效入侵检测系统提供了指导。Huang 等[9]又提出了基于数据挖掘技术的入侵检测系统，他们利用节点间属性关联性来训练神经网络，得到的模型表示了正常行为，该系统通过比较网络流量与正常模型间的差异实现异常检测。Shim 等[10]利用聚类分析技术，检测 Sinkhole 攻击。Cheng 和 Tseng[11]开发了一个可以利用当前节点上下文信息的入侵检测控制器。周永浩等[12]使用支持向量机算法对路由协议交互行为进行分析和特征提取，设计了一种分布式入侵检测系统。叶进和李伶强[13]分析了针对 MAC 层的拒绝服务攻击，提出了一个基于保护流的解决方案，指出了加入保护流的合理位置。MANET 网络入侵检测的相关综述可以参考邓立博的工作[14]。

最近，Mitrokotsa 和 Dimitrakakis[15]评估了 5 种监督学习算法在 MANET 网络入侵检测中的效果，但并未详细分析不同攻击节点及攻击比例下不同算法的性能表现。本文综合考虑了不同的攻击情况，提出了一个性能评估模型，综合考虑了算法的检测率、误报率、训练时间和检测时间，提出了一个综合评价指标，以对 7 种著名的机器学习算法进行综合量化评估。

4 基于机器学习的入侵检测方法

4.1 机器学习算法

当前，有许多机器学习算法可以用于数据分类处理。我们对本实验中使用的 7 种算法(决策树、朴素贝叶斯、多层感知器、径向基函数网络、重复增量修枝、逻辑回归及支持向量机)进行简要介绍：

决策树是重要的分类算法之一，可以高效地分类数据。它有一种树状结构，包含了一系列的决策节点(一个根节点和一系列中间节点)和叶子节点(终端节点)。每一个决策节点表示了在某个属性上的测试条件，根据输入数据的特性选择一条分支。分类过程从根节点开始，不断选择中间节点，直到叶子节点，而叶子节点包含了最后的类别信息。决策树的分类过程直观易于被人理解。C4.5 是 Quinlan 开发的一个常用的决策树工具包。

朴素贝叶斯是基于概论理论的一种简单分类算法，由贝叶斯理论推导而来，使用了极大似然估计数据的均值和方差。它假设属性间的条件独立性，实践表明这种假设并不会造成很大的精度损失。由于简单和易于实现的特性，朴素贝叶斯已经被广泛用于许多复杂问题，并工作得很好。

多层感知器也已经在很多领域中被使用。多层感知器是线性感知器的扩展版本，可以处理非线性数据。其通过反向传播算法训练神经网络，其中使用梯度下降等方法来估计权重参数。

径向基函数网络也是一种人工神经网络，与基于反向传播的神经网络一样，它也有输入层和输出层，并有几个隐藏层在两层中间。它使用径向基函数作为活化函数，学习收敛速度较快，并已经成功应用于时序分析、函数逼近、模式识别和图像处理等领域。

重复增量修枝是一个高效的规则学习算法，可以从大量有噪声的数据中学习关联规则。算法不断增加规则生成初始规则库，然后通过一系列的剪枝操作以最小化规则库的总体误差。

逻辑回归是广义线性模型的一种，多用于统计预测分析。类似于其他形式的回归模型，逻辑回归使用了一个或多个连续或离散的预测变量，利用 logistic 函数拟合数据，得到分类模型，在心理学和经济学等领域都有广泛应用。

支持向量机是当前最好的监督学习算法之一，对于小样本、非线性和高维数据都有很强的处理能力，并可扩展到其他机器学习问题如函数拟合。支持向量机方法基于统计学习理

论中的结构风险最小化原理和 Vapnik-Chervonenkis(VC)维理论，通过在训练集上进行计算，找到一个最大间隔超平面以使两个平行超平面的距离最大化。

4.2 特征模型及评估标准

本文提出一种新的评估模型来分析不同机器学习算法的性能，评估流程如图 2 所示。

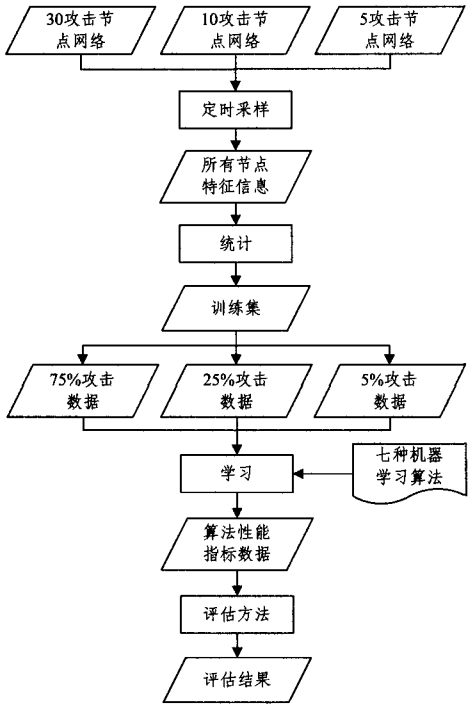

图 2 评估流程图

为了评估不同攻击情况下各种算法的检测效果，本实验设置了 3 种网络，其中的攻击节点数目分别是 30 个、10 个和 5 个。每次实验收集网络流量数据，每隔 15s 统计其中的特征数据，用于表示该采样间隔中网络活动状况。得到原始训练集后，通过调整攻击数据比例，得到攻击占比为 75%、25% 和 5%的新训练集，以更全面地评估算法性能。实验所有数据均从网络层中采集。

特征方面，我们扩展了 Mitrokotsa[15] 使用的特征，引入了 5 种新的特征，包括：丢包率(PDR)、包等待发送率(PWR)、跳数(HC)、路由数(Route Number)和坏链数(Broken Links)，定义如下：

$$PDR=\frac{Packets\ dropped}{Packets\ originated} \tag{1}$$

$$PWR=\frac{Packets\ waited}{Packets\ originated} \tag{2}$$

$$HC=\sum_{nodes}\sum_{routes}(hops\ go\ through) \tag{3}$$

$$RN=\sum_{nodes}(route\ accomplishes) \tag{4}$$

$$BLN=\sum_{nodes}(link\ failure) \tag{5}$$

通过添加这些新特征，我们希望能够捕获更多 MANET 网络中的统计信息。实验使用的全部特征定义如下：

(1)RREQ Sent：所有节点发送的 RREQ 包总数。

(2)RREP Sent：所有节点发送的 RREP 包总数。

(3)RERR Sent：所有节点发送的 RERR 包总数。

(4)RERR Re-Sent：所有节点重发送的 RERR 包总数。

(5)Data Sent：所有节点发送的 Data 包总数。

(6)Data Received：所有节点接受的 Data 包总数。

(7)Route Number：所有节点完成的路由总数。

(8)Hop Counts：所有节点完成的所有路由中经过的跳数总和。

(9)PDR：包的丢弃比率。

(10)PWR：包的等待发送队列的比率。

(11)Broken Links：网络坏链总数。

(12)Retries：网络中因坏链而产生的重试数。

实验使用标准混淆矩阵评估不同算法的检测效果。检测率(TPR)和误报率(FPR)是常用的评估标准，检测率表示正确检测出的攻击样本占总攻击样本的比率，误报率表示被错误判断为攻击的正常样本占总正常样本的比率，其定义如下：

$$TPR=\frac{TP}{TP+FN},FPR=\frac{FP}{TN+FP} \tag{6}$$

另外，我们采用 10 折交叉验证进行性能比较。首先，原始训练集被随机分为 10 个子集，然后，随机选择一个子集为测试集，余下的 9 个子集作为训练集训练模型。该过程重复 10 次，最后对 10 次的结果进行平均得到最终分析结果。

根据统计得到的 TPR、FPR、模型的检测及建模时间，我们提出了一个综合评价指标 TotalScore，定义如下：

$$TotalScore=\frac{TPR*(1-FPR)}{TPR+1-FPR}-\frac{detecting\ time}{100}-\frac{training\ time}{1000000} \tag{7}$$

该指标为每一个机器学习算法给出了一个综合评价，TPR 越高，FPR 值越低，检测时间及训练时间越低，综合指标值就越高。

5 实验

5.1 模拟环境

本实验使用 GloMoSim 模拟一个 MANET 网络，表 1 展示了实验各项参数。我们模拟了一个 $2000\times2000m^2$ 网络，50 个节点随机分布于其中。每个节点的无线传输范围(Radio Propagation Range)为 250m，信道容量(Channel Capacity)为 2Mb/s。每个节点发送固定比特率(Constant Bit Rate)应用层数据包，包大小从 128bytes 到 1024bytes 不等。路由协议为 Ad hoc On Demand Distance Vector。节点按照 Random Way Point 模型移动，等待时间被设置为 0，30，50，100 和 400s，在该配置下，每一个节点随机选择一个目的地并移动，到达目的地后，节点停留一个等待时间，然后继续随机选择目的地并移动。每次实验模拟 1000s 网络运行时间。

表 1 模拟参数

参数名	取值/选择
Communication type	CBR
Routing protocol	AODV
Number of nodes	50
Node placement	Random
Mobility	Random way point
Minimum speed	0m/s
Maximum speed	10，20 and 30m/s
Simulation area	2000m×2000m
Pause time	0，30，50，100 and 400s
Radio Transmission power	15dBm
Channel capacity	2Mb/S
Simulation time	1000s
Number of malicious nodes	30，10 and 5
Sampling periods	15s

通过修改节点最大移动速度(10，20 和 30m/s)和暂停时间(0，30，50，100 和 400s)，我们创建一系列的实验数据集，统

计采样间隔为 15s。模拟一种攻击类型，每次采样后的统计数据被标记为 4 种类型：NORMAL，FLOODING，BLACKHOLE 和 PACKETDROP。最后，我们把所有标记数据混合在一起得到训练集。

机器学习工具使用开源工程 WEKA。实验硬件环境是 Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz，2GB 内存。

5.2 实验结果

我们共进行 180 次实验模拟不同参数下的网络运行情况，生成原始数据集，攻击节点数分别设置为 30 个、10 个和 5 个，流量数据中包含了 3 种攻击类型和 1 种正常类型。在 180000s 的模拟时间中，对 50 个节点进行采样，得到 11664 条记录，具体实验生成原始数据集见表 2。对于在每一种攻击节点数下生成的入侵数据，调整攻击数据比例为 75%、25% 和 5%，得到 9 个不同的训练集用于检测和分析。对于每种机器学习算法，我们调整相应的学习参数，进行一系列实验，选择具有最低检测误差的参数组合。最后对 9 个训练集上实验得到的 TPR 和 FPR 进行算术平均，得到实验结果图。

表 2 实验原始数据(条)

攻击节点数	丢包	洪水	黑洞	正常
30	980	990	990	/
10	989	947	990	/
5	924	990	990	/
0	/	/	/	2874

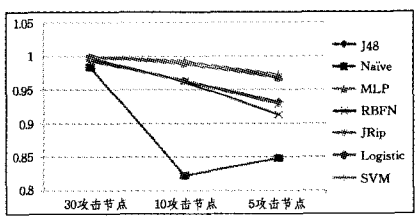

图 3 不同攻击节点平均 TPR

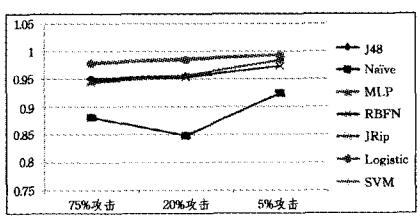

图 4 不同攻击比例平均 TPR

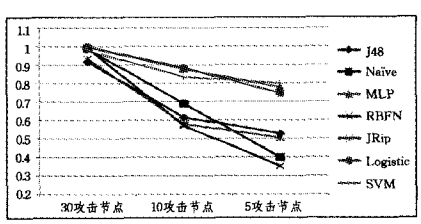

图 5 不同攻击节点下丢包攻击平均 TPR

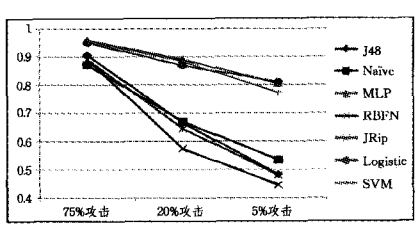

图 6 不同攻击比例下丢包攻击平均 TPR

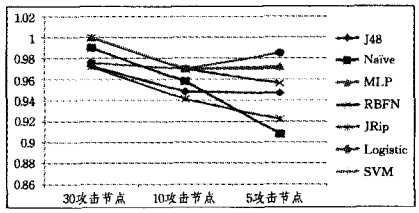

图 7 不同攻击节点下洪水攻击平均 TPR

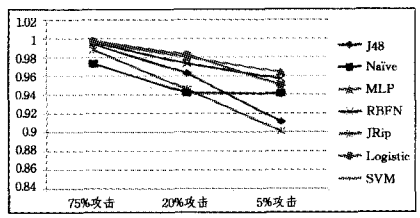

图 8 不同攻击比例下洪水攻击平均 TPR

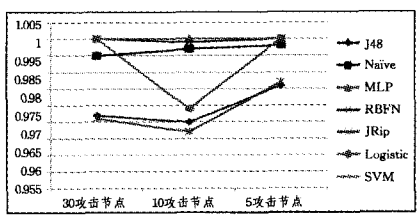

图 9 不同攻击节点下黑洞攻击平均 TPR

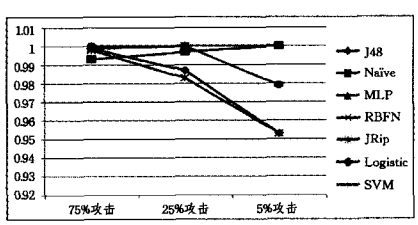

图 10 不同攻击比例下黑洞攻击平均 TPR

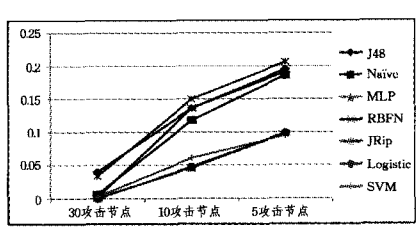

图 11 不同攻击节点平均 FPR

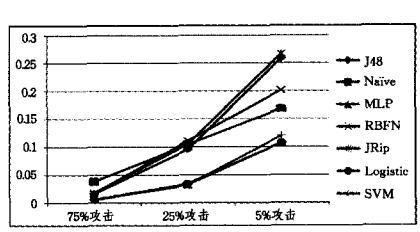

图 12 不同攻击比例平均 FPR

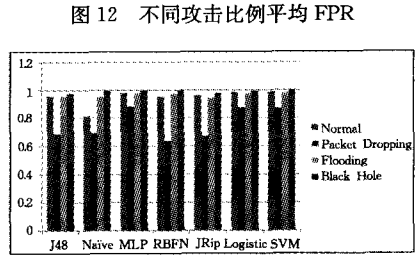

图 13 每种类型平均 TPR

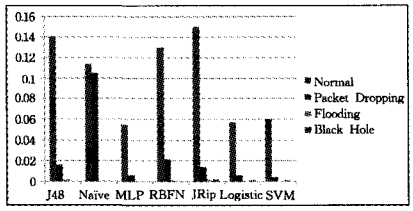

图 14　每种类型平均 FPR

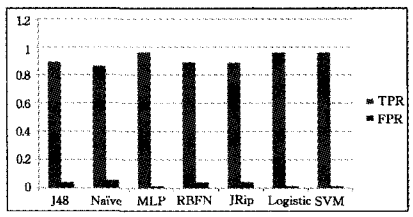

图 15　每种机器学习算法总体平均 TPR 和 FPR

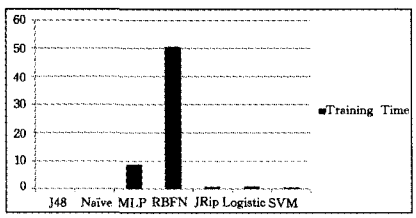

图 16　每种机器学习算法平均训练时间

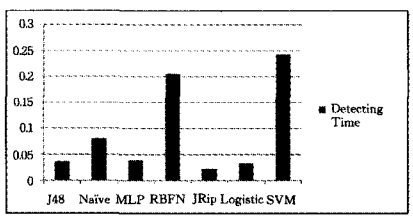

图 17　每种机器学习算法平均检测时间

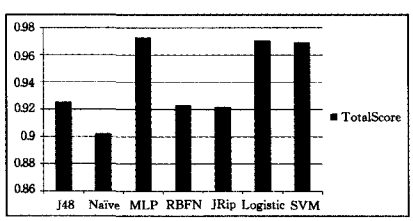

图 18　每种机器学习算法综合性能指标

图 3、图 4 展示了不同攻击节点数及攻击比例下每一种机器学习算法的平均 TPR，图 5、图 6 展示了不同攻击节点数及攻击比例下丢包攻击的平均 TPR，图 7、图 8 展示了不同攻击节点数及攻击比例下洪水攻击的平均 TPR，图 9、图 10 展示了不同攻击节点数及攻击比例下黑洞攻击的平均 TPR。可以看到，多层感知器、支持向量机和逻辑回归有较高的 TPR，随着攻击节点和网络中攻击比例的减少，这 3 种机器学习算法的 TPR 普遍要比其他算法更高。图 11、图 12 展示了不同攻击节点数及攻击比例下每一种机器学习算法的平均 FPR，可以看到，当攻击节点数较多、攻击比例较大时，所有算法 FPR 值都较低，但随着攻击节点或攻击比例的减少，多层感知器、支持向量机和逻辑回归仍然具有较低的 FPR。图 13 展示了所有算法对每一种类型的平均 TRP，图 14 展示了所有算法对每一种类型的平均 FRP，图 15 展示了所有算法的总体平均 TPR 及 FPR，多层感知器、支持向量机和逻辑回归具有最高的平均 TPR 及最低的平均 FPR，图 16 表示了所有算法的平均训练时间，上述 3 种算法中，多层感知器花费 8.744s 训练分类模型，而支持向量机、逻辑回归分别平均只花费 0.424s、0.932s 的时间建模。图 17 表示了所有算法的平均检测时间，每一种算法花费时间都很少，不超过 0.25s。图 18 给出了所有算法的综合评价指标值，可以看到，多层感知器、支持向量机和逻辑回归的综合表现要优于其他算法。

结束语　本文研究 MANET 网络可能遭遇的攻击方式，提出了一种基于机器学习技术的入侵检测性能评估模型，建立了刻画网络流量的特征模型，提出了一个综合评价指标，对 7 种著名的机器学习算法在 MANET 网络入侵检测中的效果进行了分析。实验模拟了丢包、洪水和黑洞 3 种入侵行为，仿真工具采样原始流量数据并统计得到训练集，用于机器学习算法训练分类模型。实验结果显示，该入侵检测性能评估模型能较好地刻画 MANET 网络中的入侵行为，为机器学习算法提供较好的分类效果，给出了不同网络攻击情况下不同算法的检测效果。提出的综合评价指标能较好地综合反映算法的各项性能指标，结果显示，多层感知器、逻辑回归和支持向量机具有最高的检测率及最低的误报率，且训练时间及检测时间都较少，相比其他算法更适用于 MANET 网络的入侵检测工作。将来的工作主要着重于进一步研究这 3 种算法，如利用 Boosting 等技术构建强分类器并建模和仿真，以建立一个高效的 MANET 入侵检测系统。

参 考 文 献

[1] Indirani G, 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, 2013 (ahead-of-print): 1-14

[2] Mechtri L, Djemili F T, Ghanemi S. On the Design of a New Intrusion Detection System for Securing MANET: An Agent-Based Approach[J]. International Journal of Advanced Computer Science, 2013, 3(6)

[3] Tripathi S S, Agrawal S. A Survey on Enhanced Intrusion Detection System in Mobile Ad-hoc Network[J]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2012, 1(7): 44-48

[4] Kahn R. The organization of computer resources into a packet radio network[J]. Communications, IEEE Transactions on, 1977, 25(1): 169-178

[5] Jubin J, Tornow J D. The DARPA packet radio network protocols[J]. Proceedings of the IEEE, 1987, 75(1): 21-32

[6] Anderson J P. Computer security threat monitoring and surveillance[R]. James P. Anderson Company, Fort Washington, Pennsylvania, 1980

[7] Denning D E. An intrusion-detection model[J]. Software Engineering, IEEE Transactions on, 1987(2): 222-232

[8] Zhang Y, Lee W, Huang Y A. Intrusion detection techniques for mobile wireless networks[J]. Wireless Networks, 2003, 9(5): 545-556

[9] Huang Y, Lee W. A cooperative intrusion detection system for ad hoc networks[C]//Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. ACM, 2003: 135-147

(下转第 191 页)

当密文格式正确且是合法用户发送的信息时，主会场才能成功解密出会话密钥。

与传统加密算法相比，多对一加密算法的多个发送者共享一台服务器上的密钥来解密，服务器密钥存储量远远少于发送者的数量，也就是说仅仅使用唯一的密钥可以对所有的发送者的密文进行解密和认证，当合法发送者数目非常大时，就可以避免接收者保存大量认证密钥和发送者名单，因此大大减少了接收者的计算时间和存储空间，节省了系统的开销，密钥的管理也更简单，减轻了其负担，服务器只需要保存主密钥就能解密根据用户身份加密后的密文。

视频会议的安全需求主要体现在[8,9]：身份认证、数据完整性、私密性、不可抵赖性。多对一加密认证算法使用了用户的身份信息产生加密密钥，只有合法用户传送的会话密钥才能被主会场正确解密；数据完整性：使用二次加密保证了会话密钥的安全，两个端点之间进行通信的有效数据不被损坏或篡改，数据完整性得到保证；私密性：即使传送的数据被图谋不轨的人截获，在不知道解密算法和密钥的情况下仍然无法获取有效信息。不可抵赖性：由于多对一加密认证算法的加解密过程是基于身份认证的，防止了发送方和接收方抵赖其所传输的数据。

3.3 算法安全性证明

首先假设存在一个算法 δ 可以伪造密文，则构造算法 β 可以攻破该方案[10-13]，预先选取散列函数 $SHA1$，发送者身份和接收者身份组成序列对 (ID_A, ID_S)，将该问题的参数 (G, F, P, xP, yP, zP, e) 和 $T \in F$ 发送给 β，如果 $e(P,P)^{xyz}=T$，则返回值为 1，否则返回值为 0，算法 δ 作为子程序被算法 β 调用，证明过程如下：δ 发送两个等长的消息 $M0, M1$ 以及身份给 β 作为挑战，如果 ID_i 已经被分配，β 失败，否则，β 做如下计算：若 ID_i^* 没有被分配，则令 $ID_i^*=ID_A^*$，随机选取 $\beta \in \{0,1\}$ 和 $r_1 \in Z_P^*$，(r_1P, M_β) 没有在 $SHA1$ 查询中被查询；通过在 $SHA1\text{-}list$ 中计算 $SHA1(ID_I)$ 获得 θ，通过输入 ID_i 调用 $Information\text{-}Extract$ 得到 $Info_i$，然后计算 $\gamma=SHA1(Info_I, ID_A^*)$、$c^*=r_1P$、$v^*=M_\beta \oplus H(T^{\theta\gamma})$ 和 $u^*=\frac{1}{H_1(ID_A^*)+s}(\theta zP+r_1\theta P)$，最后输出 $C^*=(c^*, u^*, v^*)$ 作为挑战密文。通过推理验证可得到 $u^*=(z+r_1)EK_1$：

$$
\begin{aligned}
u^* &= \frac{1}{H_1(ID_A^*)+s}(\theta zP+r_1\theta P)\\
&= \frac{z+r_1}{H_1(ID_A^*)+s}Q_i\\
&= (z+r_1)EK_1
\end{aligned}
$$

并且可得到：

$$
\begin{aligned}
v^* &= M_\beta \oplus H(T^{\theta\gamma})\\
&= M_\beta \oplus H(\hat{e}(xP, yP)^{\theta yz})\\
&= M_\beta \oplus H(Info_I^{xz})\\
&= M_\beta \oplus H(EK_2^z)
\end{aligned}
$$

$EK_{A,I}=(EK_1, EK_2)$ 作为回应 (ID_A^*, ID_I) 的加密密钥，并且我们隐含地定义 $z=H_2(c^*, M_\beta)$，如果 $T=\hat{e}(P,P)^{xyz}$，那么 C^* 是合法的明文。

结束语 本文针对视频会议安全保密系统中密钥容易泄露的问题，在现有加密解密算法的基础上提出了使用基于椭圆曲线的多对一加密认证的方案设计视频会议安全机制，其优势是能够减轻服务器存储和管理密钥的负担，大大节省了服务器的存储空间。该方案不仅保证了通信数据的机密性和完整性，而且能够保证参加会议人员身份的真实性。随着加密解密算法的不断改进，其必将有更广阔的应用前景。

参 考 文 献

[1] Al-Riyami S S, Paterson K G. CBE from CL-PKE: A generic construction and efficient schemes [C]// LNCS 3386: PKC 2005. Berlin: Springer, 2005: 398-415

[2] 唐楚华. 视频会议系统的研究与实现[D]. 武汉：武汉理工大学，2011

[3] 邓秀峰，赵明生. 一种基于 SIP 的视频会议安全机制[J]. 计算机工程，2004，30(8)：106-108

[4] 李星，郭穗鸣，等. 可扩展分布式标清视频会议系统：结构和转发模型[J]. 清华大学学报，2012，52(9)：1275-1280

[5] 林喜军，孙琳，武传坤. 基于双线性映射的多对一加密认证方案[J]. 计算机研究与发展，2009(02)

[6] 邹永辉，严亚俊，等. 椭圆曲线密码体制的实现及发展现状简介[J]. 计算机时代，2005(1)

[7] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全(第二版)[M]. 北京：清华大学出版社，1998

[8] 徐彦彦，徐正权，等. 视频会议系统安全体系设计[J]. 计算机工程与应用，2006，14：208-211

[9] Phong L T, Matsuoka H, Ogata W. Stateful Identity-Based Encryption Scheme: Faster Encryption and Decryption [C]// ASIACCS' 08. Tokyo, Japan, March 2008

[10] Yao Hua-zhen, Jing Ya-tao. The Design of Video-Conference Encryption System based on H. 264. 978-1-4244-7874-3/10© 2010 IEEE

[11] Lin Xi-jun, Wu Kun-chuan, Liu Feng. Many-to-one encryption and authentication scheme and its application [J]. Journal of Communications and Networks, 2008, 10(1)

[12] Shamir A. Identity-based cryptosystems and signature schemes [C]// LNCS 196: CRYPTO 1984. Berlin: Springer, 1985: 48-53

[13] Purdy G B. A High Security Log-in Procedure[J]. Communications of the ACM, 1974, 17(8): 442-445

(上接第 174 页)

[10] Shim W, Kim G, Kim S. A distributed sinkhole detection method using cluster analysis[J]. Expert Systems with Applications, 2010, 37(12): 8486-8491

[11] Cheng B C, Tseng R Y. A context adaptive intrusion detection system for MANET[J]. Computer Communications, 2011, 34(3): 310-318

[12] 周永浩，李鸥，刘洋. 基于 SVM 的 MANET 路由层入侵检测[J]. 计算机应用研究，2010，27(5)

[13] 叶进，李伶强. 基于保护流的 MANET 网 MAC 层 DoS 攻击及防御[J]. 计算机科学，2011，38(4)：118-121

[14] 邓立博. MANET 入侵检测系统研究与实现[D]. 哈尔滨：哈尔滨工程大学，2012

[15] Mitrokotsa A, Dimitrakakis C. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection[Z]. Ad-hoc Networks, 2012