无线Mesh网络基于隐半马尔可夫模型的跨层结合异常检测方法

王 涛[1] 吴晓燕[2] 程良伦[1]
(广东工业大学自动化学院 广州 510006)[1] (四川文理学院计算机科学系 达州 635000)[2]

摘 要 目前无线Mesh网络异常检测的方法大多针对单一恶意攻击,还不具备检测来自不同协议层的恶意攻击的综合能力。提出一种基于多协议层跨层结合的异常检测方法,即采集多协议层结合的特征对网络运行状态进行全方位监测,并训练隐半马尔可夫模型对网络正常运行状态进行描述,通过计算多维观测序列相对于隐半马尔可夫模型的熵来评价其"正常性",从而发现源自不同协议层的恶意攻击行为。实验仿真证明,该方法能有效检测源自各协议层的多种恶意攻击,具有一定的通用性。

关键词 无线Mesh网络,跨层结合,观测序列,隐半马尔可夫模型,异常检测
中图法分类号 TP393 **文献标识码** A

Cross-layer Based Anomaly Detection Mechanism with Hidden Semi-Markov Model in Wireless Mesh Networks

WANG Tao[1] WU Xiao-yan[2] CHENG Liang-lun[1]
(Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China)[1]
(Department of Computer Science, Sichuan University of Arts and Science, Dazhou 635000, China)[2]

Abstract The existing methods on anomaly detection in wireless Mesh network mostly focus on single malicious attack, which can not detect various malicious attacks originated form different protocol layers. We presented a cross-layer based anomaly detection mechanism. Firstly a distributed IDS structure for Mesh backbone network topology was proposed, secondly cross-layer based features were collected for comprehensively monitoring network activities. Furthermore, with the multidimensional observation sequences, the hidden semi-Markov model(HsMM) was trained and exploited to characterize and model the normal states of network activities. The entropies of observation sequences against the HsMM were calculated to evaluate their abnormality. An anomaly alert will be reported if the entropy is lower than a threshold. Experiment results show that the proposed detection mechanism is able to detect various malicious attacks from different protocol layers.

Keywords Wireless Mesh network, Cross-layer based, Observation sequences, Hidden semi-Markov model, Anomaly detection

1 引言

无线Mesh网络是一种高容量、高速率的分布式网络。它由Mesh路由器节点组成高健壮性的网格状骨干网络,利用多跳路由机制增加网络覆盖的灵活性,从而实现各种异构无线子网的高效无缝接入。无线Mesh技术是未来无线城域网理想的组网方式,并且是各种异构无线网络的融合与协同的关键技术。然而,由于无线通信信道的开放性,其容易受到干扰、监听、消息重放、报文篡改等各种攻击,随着无线Mesh网络的普遍应用,其安全问题将非常突出。

现有部分研究利用加密与认证技术来加强无线Mesh网络通信安全,ZHANG等人[1]提出一种攻击容忍的安全架构;WANG等人[2]提出一种组密钥管理框架加强组通信安全。然而,仅仅利用加密与认证技术难以充分有效地保证无线Mesh网的安全,尤其是难以防范来自于内部被俘获节点的或针对网络性能(如泛洪攻击、通信干扰等)的恶意攻击。因此,利用入侵检测作为安全的第二道保护屏障,在无线Mesh网络中非常必要。

无线网络入侵检测研究,多数是针对无线网络中某种具体的攻击手段进行防御,比如黑洞攻击[3]、拜占庭攻击[4]、拒绝服务攻击[5]等,其检测性能比较单一,通常只能较好地检测单一协议层上的入侵行为。为此,研究人员引入跨层协作机制,以优化网络的通信与安全性能。BOSE S.等人[6]提出无线自组织网络中一种多层结合的入侵检测系统,其利用采集

到稿日期:2011-09-22 返修日期:2011-11-24 本文受国家自然科学基金-广东省联合基金重点项目(U0935002),广东省重大科技专项(2009A080207008),广州市科技计划项目(2010Z1-D00061),广东省高校优秀青年创新人才培养计划项目(LYM11057)资助。
王 涛(1983—),男,博士,主要研究方向为无线网络安全、传感器网路,E-mail:wangtaosea@msn.com;吴晓燕(1981—),女,讲师,主要研究方向为网络技术;程良伦(1964—),男,教授,博士生导师,主要研究方向为传感器网络、网络测量等。

自多协议层的特征检测可能存在的恶意攻击。进一步，BOSE S. 等人[7]提出利用跨层入侵检测模型发现拒绝服务攻击，相比于传统入侵检测模型其具有更高的准确性。JOSEPH 等人[8]提出利用跨层结合特征以及机器学习算法检测无线自组织网络中的异常汇聚行为。THAMILARASU 等人[9]提出利用博弈论模型结合跨层特征检测干扰攻击。可见，上述研究尽管引入了跨层机制，但还只是用于提高检测的准确率，并且其检测对象还只是局限在某种安全攻击，未能提出一种能有效检测源于不同协议层恶意攻击的方法。

另外，上述相关研究都是关注无线自组织网络中的入侵检测问题，而目前在 WMNs 入侵检测领域的研究成果还很少。无线 Mesh 网络与自组织网络具有较多相同的特性，如分布性、无线多跳通信等。然而，相对于无线自组织网络，无线 Mesh 网络具有更大的网络规模，其接入终端数量众多且种类各异，在所有终端直接部署 IDS 难以实现并会带来巨大的系统负荷；另外，无线 Mesh 网络具有独特的网络拓扑架构，也需要研究相适应的入侵检测架构。

由于无线网络中计算、存储等资源的匮乏，为每种恶意攻击单独设计一种检测方法不太现实，因此有必要研究具有一定通用性和多种恶意行为检测能力的异常检测方法。针对现有研究检测能力单一与无线 Mesh 网络特点，本文提出一种无线 Mesh 网络中跨层协作的异常检测方法，即通过采集多协议层结合的特征并评估其"正常性"来发现源自不同协议层的多种恶意攻击行为。为了有效描述网络正常行为与状态，本文采用隐半马尔可夫模型（Hidden semi-Markov Model，HsMM）[13]描述无线 Mesh 路由器覆盖范围内节点通信行为的随机变化过程（如移动状态、跨区漫游、通信负载变化、断链与恢复等）。隐马尔可夫模型（Hidden Markov Model，HMM）已经在语音识别、手写体/文字识别、数字通信编解码、DNA 序列分类等许多重要领域获得了广泛和成功的应用[11]。隐马尔可夫模型常用于随机过程建模，但要求状态的持续时间服从几何、指数等规则分布。与 HMM 相比，HsMM 更适合描述状态持续时间为任意分布的隐马尔可夫过程。利用网络正常运行时采集的多维观测序列训练估计 HsMM 模型参数，通过计算多维观测序列相对于已训练 HsMM 模型的熵来评价其"正常性"，若其熵值超过某个阈值，则可认为出现异常。

2 恶意攻击与特征选择

2.1 恶意攻击

在无线 Mesh 网络中，恶意攻击一般可以分为被动攻击与主动攻击。被动攻击主要指网络流量窃听，这种攻击难以检测，但通常是攻击者发起主动攻击的前奏。攻击者一旦获取了足够的信息，就可发起主动攻击。主动攻击可在各个协议层上发起，可针对网络通信协议、带宽资源、数据可用性与完整性等各种对象。典型的攻击方式如表 1 所列。

物理层容易受到干扰攻击，攻击者通过较强的噪声信号来干扰或掩盖正常用户的信号传输，从而达到对物理信道进行攻击的目的。在 MAC 层与网络层，恶意攻击形式比较多样，如泛洪攻击、睡眠剥夺攻击在 MAC 层与网络层都可以发起。在网络层，攻击者还可以发起黑洞攻击、虫洞攻击、路由协议攻击。在黑洞攻击中，攻击者广播伪造的路由控制信息，比如在按需路由协议中，宣称自己是到达某目的节点的最佳路径，从而中途截获所有传送给目的节点的数据包。虫洞攻击是指两个串通的恶意节点彼此间建立一条私有通道，攻击者在网络中的一个位置上记录数据包的信息，利用此私有通道将窃取的信息传递到网络的另外一个位置，造成数据包的丢失或破坏；同时私有通道能够造成比实际路径短的虚假路径，扰乱节点间的路径选择，从而导致路由发现过程的失败。路由协议攻击是指攻击者通过广播大量路由控制包来破坏路由表、扰乱网络正常通信。

表 1 各协议层恶意攻击

Layer	Malicious Attack
Physical Layer	Jamming
MAC Layer	flooding, sleep deprivation, identity theft, DoS, spoofing
Network Layer	flooding, sleep deprivation, packet dropping, spoofing, black-hole, wormhole, routing protocol attack

面临种类各异的恶意攻击，目前异常检测研究主要是针对某种单一恶意攻击进行检测，其主要原因之一在于这些检测模型所提取的观测值比较单一。为建立一种比较通用的检测模型，我们提出使用跨层结合的异常检测方法，从物理层、MAC 层、网络层提取观测值，通过跨层观测序列建立网络正常行为模型，并以此检测各种恶意攻击行为。

2.2 跨层特征选择

每种攻击都有其特定的行为模式，一定程度上会造成网络运行状态的偏离或异常。为检测各种恶意攻击，需研究其行为特征并分析选取与其密切相关的观测特征。如检测物理层干扰攻击，可以选取接收信号强度-RSS（Received Signal Strength）、信道切换频率等。在 MAC 层，泛洪攻击、剥夺睡眠攻击、DoS 攻击通常会导致 NAV、重传 RTS 控制包数量、链路丢失率的变化。在网络层，采用分组流量以及路由缓存相关的特征，前者包括接收到的数据分组、路由请求、路由响应以及路由错误包的数量，后者包括路由添加、修改的比率。我们选取的跨层结合的观测特征如表 2 所列。

表 2 跨层结合的特征集合

Layer		Selected observations	Sampling periods
Physical Layer		RSS, Channel switching frequency	5 seconds
MAC Layer		NAV, reXmitRTS, Link Loss rate	
Network Layer	Traffic related	Recv_packet, Route request, Route reply, Route error	
	Link cache related	Link added, modified; Route changed	

但需注意到，选取的某些观测特征之间并非独立无关的，某种恶意攻击可能会导致某些观测对象同时发生变化。比如泛洪攻击会带来 reXmitRTS、Link loss rate、Recv_packet 等观测值的同时变化，说明这些特征间有一定的相关关系。由于特征数量过多会增加检测模型训练的复杂度，因此为减少特征维度与冗余度，本文采用主成分分析方法[12]对特征向量进行降维处理，将原有特征重新组合成一组新的互相无关的几个综合特征。算法原理如下：

在第 t 次采样时，表 2 中各个协议层的观测值组成一个多维的观测值向量：$\bar{o}_t=(f_{1t},f_{2t},\cdots,f_{Nt})^T$，其中 $f_{1t},f_{2t},\cdots,$

f_N 代表各个观测特征在时刻 t 的数值。那么，T 次采样后平均观测向量为

$$\vec{\mu}=\frac{1}{T}\sum_{t=1}^{T}\vec{o}_t \tag{1}$$

观测向量相对于平均向量 $\vec{\mu}$ 的偏离可表示为

$$\vec{\phi}_t=\vec{o}_t-\vec{\mu}$$

那么样本的协方差矩阵则为

$$C=\frac{1}{T}\sum_{t=1}^{T}(\vec{o}_t-\vec{\mu})(\vec{o}_t-\vec{\mu})^{\mathrm{T}}=\frac{1}{T}\sum_{t=1}^{T}\vec{\phi}_t\,\vec{\phi}_t^{\mathrm{T}}=\frac{1}{T}\varphi\varphi^{\mathrm{T}} \tag{2}$$

式中，$\varphi=[\vec{\phi}_1\ \vec{\phi}_2\cdots\vec{\phi}_T]$。假设 $(\lambda_1,u_1),\cdots,(\lambda_N,u_N)$ 是该矩阵的 N 对特征值与特征向量，我们选取最大的 K 个特征值及其对应的特征向量作为主成分，并满足如下条件，即

$$\sum_{i=1}^{K}\lambda_i/\sum_{i=1}^{N}\lambda_i\geqslant\alpha \tag{3}$$

式中，α 预先给定，表示主成分的累计贡献率。进一步，K 个特征向量组成 $N\times K$ 维的本征矩阵 U，并求得映射到 K 维子空间的主成分为

$$\vec{a}_t=U^{\mathrm{T}}(\vec{o}_t-\vec{\mu})=U^{\mathrm{T}}\vec{\phi}_t,t=1,\cdots,T \tag{4}$$

3 异常检测

3.1 HsMM 算法

在网络正常运行时，观测序列代表观测某无线 Mesh 路由器节点覆盖范围内的正常网络行为与环境状态，并受到各种潜在因素的影响，如接入节点跨区移动通信、网络通信负载动态变化以及无线网络环境等。可将这些潜在的因素定义为网络的状态，且使其不易被直接观测。对每个给定的状态，由于这些潜在的因素不确定，因此对应有不同的观测值向量。由于这些隐藏状态的持续时间是任意分布的，因此可以认为随机过程为一个隐半马尔可夫过程，其 Markov 状态（隐状态）对应节点周围的网络行为与环境。HsMM 的隐状态之间的转移关系，代表观测节点自身以及周围网络运行状态的变换，比如网络通信负载、延迟、路由更新等。HsMM 模型的具体定义如下：

(1) $S=\{1,\cdots,M\}$ 是正常节点网络行为可能的隐状态集合，M 是状态数。M 状态的马尔可夫链的状态转移矩阵为 $A=[a_{mn}]_{M\times M}$，其中 a_{mn} 是由状态 m 转移到状态 n 的概率，$m,n=1,\cdots,M$。即 $a_{mn}=\Pr[q_t=n\mid q_{t-1}=m]$，$m,n\in S$，$q_t$ 表示 t 时刻的状态。(2) 假定每个状态的持续时间为任意分布，$p_m(d)=\Pr[\tau_t=d\mid q_t=m]$，$\tau_t$ 表示当前状态 q_t 将持续的次数，$d\in\{1,\cdots,D\}$，D 是状态驻留的最大次数，且满足 $\sum_d p_m(d)=1,d\in\{1,\cdots,D\}$，定义状态驻留矩阵 $P=[p_m(d):m\in S,d=1,\cdots,D]$。(3) 定义在给定状态 m 时，模型的输出概率分布为 $b_m(k)=\Pr[o_t=k\mid q_t=m]$，其中 $m\in S$ 且 $k\in V=\{1,\cdots,K\}$，K 表示模型输出符号的个数，o_t 为 t 时刻的观测值。输出概率满足 $\sum_k b_m(k)=1,k\in V,m\in S$。定义输出概率矩阵 $B=[b_m(k):k\in V,m\in S]$。(4) π 是初始状态概率矩阵，$\pi_m=\Pr[q_1=m],m\in S$，初始状态概率分布满足 $\sum_m\pi_m=1,m\in S$。因此，HsMM 的模型参数 λ 包括转移概率矩阵 A、状态驻留概率矩阵 P、输出概率矩阵 B 以及初始状态概率矩阵 π，记为 $\lambda=(A,P,B,\pi)$。本文使用此模型来描述节点正常的网络行为，并检测异常节点。我们采集正常情况下的观测数据来训练模型参数，HsMM 模型参数训练估计算法见文献[12]。在得到描述节点正常行为的 HsMM 模型后，即可用于检测网络中的异常行为。本地节点计算采集的多维观测序列对于 HsMM 检测模型的熵，如果低于某个阈值，则认为可能存在异常行为，并发起与周围邻近节点的联合检测过程。

本文依照下面算法来计算观测序列对 HsMM 模型的或然概率。假定 o_1^t 表示由时刻 1 到 t 的观测序列，我们定义

$$\alpha_t(m,d)=\Pr\{q_t=m,\tau_t=d\mid o_1^t,\lambda\} \tag{5}$$

式中，q_t 表示 t 时刻的状态，τ_t 表示当前状态 q_t 还将持续的次数。$\Pr\{q_t=m,\tau_t=d\mid o_1^t,\lambda\}$ 表示在给定观测序列 o_1^t 以及模型 λ 时，在 t 时刻状态是 m 的概率。定义

$$\alpha_t^*(m,d)=\Pr\{q_t=m,\tau_t=d,o_1^t\mid\lambda\} \tag{6}$$

结合上面两式，则有

$$\alpha_t(m,d)=\frac{\alpha_t^*(m,d)}{\Pr\{o_1^t\mid\lambda\}}=\frac{\alpha_t^*(m,d)}{\sum_{m,d}\alpha_t^*(m,d)} \tag{7}$$

我们使用 HsMM 前向算法[13]来计算或然概率 $\Pr\{o_1^t\mid\lambda\}$。假如此或然概率低于阈值，则发现异常行为。迭代估计算法包括下面几个步骤：

(1) 初始状态：$\alpha_0^*(m,d)=\pi_m p_m(d)$，for $m\in S,d\geqslant 1$。

(2) 在时刻 t，根据已有的前向变量迭代结果 $\alpha_{t-1}^*(m,d)$，$m\in S$，以及当前观测值 o_t，则 t 时刻的前向变量为

$$\begin{aligned}\alpha_t^*(m',d')&=\sum_{m\in s,d\geqslant 1}\Pr\{q_{t-1}=m,\tau_{t-1}=d,q_t=m',\tau_t=d',o_1^t\mid\lambda\}\\&=(\alpha_{t-1}^*(m',d'+1)+\sum_{m\in S,m\neq m'}\alpha_{t-1}^*(m,1)a_{mm'}p_{m'}(d'))b_{m'}(o_t)\end{aligned} \tag{8}$$

(3) 观测序列 o_1^t 对模型 λ 的或然概率为

$$\Pr\{o_1^t\mid\lambda\}=\sum_{m,d}\alpha_t^*(m,d) \tag{9}$$

进一步，观测序列对模型的熵为

$$Entropy=\ln\Pr\{o_1^t\mid\lambda\}/t \tag{10}$$

此异常检测算法可用于在线实时检测，只需要保存上一次的迭代结果，而当前观测值只需在前向递归过程中使用一次且不用保存。对无线移动网，可以有效节省移动 IDS 主机的存储空间，降低运行负荷，并能及时发现入侵行为。

3.2 异常检测模型

无线 Mesh 网络包含由 Mesh 路由器构成的网状骨干网以及各种异构接入子网。Mesh 路由器位置相对固定并拥有较强的计算能力，可以作为部署 IDS-Agent 的平台，称为 MR IDS-Agent。本文提出异常检测模型整体流程，如图 1 所示。模型训练阶段包括两个部分：

1) 基于主成分分析的数据变换与降维

a) 计算训练集中样本矩阵的平均矩阵、差分矩阵以及协方差矩阵；

b) 计算协方差矩阵特征值、特征向量；

c) 按特征值由大到小进行排序，取较大的 K 个特征值以及特征向量，本文中取 $\alpha=80\%$；

d) 基于选取的 K 个特征向量构建本征矩阵 U，并将原有 N 维训练集变换为 K 维（$K<N$）不相关的主成分训练集。

2) HsMM 模型训练

a) 利用经主成分分析变换后的训练集估计 HsMM 模型参数，训练算法见 3.1 节；

b) 计算训练集中观测序列相对于 HsMM 的熵，基于熵的概率分布获取熵的阈值，用于判断异常。

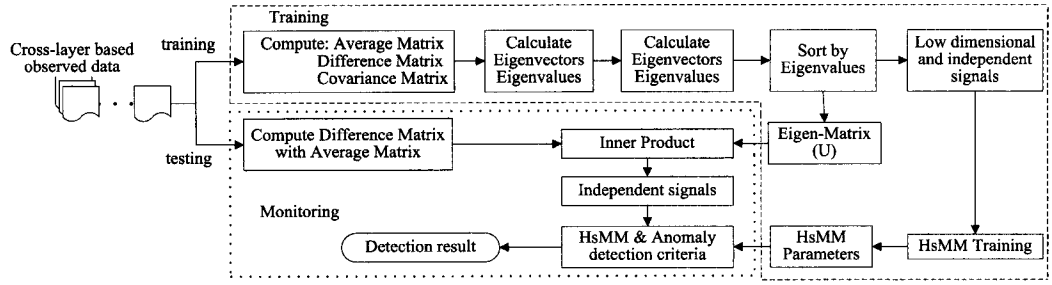


图 1　MR IDS-Agent 异常检测结构

异常检测模型的监测阶段包括以下步骤：

1)计算测试观测集样本矩阵的平均矩阵及其差分矩阵；

2)利用本征矩阵 U,对观测集样本差分矩阵进行主成分分析变换；

3)计算各变换后的观测序列相对于 HsMM 模型的熵,与阈值进行比较并判断其异常程度。

4　实验结果

4.1　实验环境

本文使用 ns-2 作为实验仿真平台,仿真网络拓扑如图 2 所示。上层为 Mesh 路由器节点组成的网状骨干网,下层为自由移动的漫游节点。

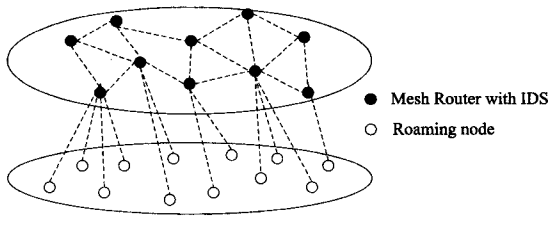


图 2　仿真网络拓扑

本文仿真实验参数设置如表 3 所列。

表 3　仿真参数设置

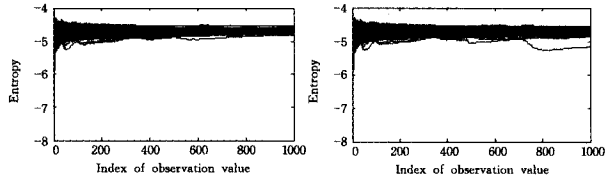
网络参数	数值
拓扑范围	1km×1km
Mesh 路由器节点数量	30
Mesh 路由器节点通信距离	500m
Mesh 骨干网路由协议	DSR
漫游节点移动模式	Random Waypoint Model
漫游节点停留时间	100s
漫游节点数量	100
漫游节点移动速率	Normal(5,1)
漫游节点通信距离	300m
流量数量	15
流量数据速率	4packets/s,512bytes/packet
仿真时间	2h
取样间隔	1s

在仿真过程中,设置上层 Mesh 路由器节点数量为 30 个,分布在 1km×1km 区域内,Mesh 路由器节点运行 DSR 路由协议。下层漫游节点移动模式设置为 Ramdom Waypoint Model,节点从一个随机起点向某个随机目的点移动,到达目的点后停留一段时间,本仿真场景中为 100s。节点的移动速率分布服从正态分布 normal(5,1)。同时,配置网络背景流量,选取 15 个节点以恒定速率向随机的目的节点发送数据。每个 Mesh 路由器节点部署 IDS 模块,负责监测各自覆盖区域内节点的网络通信行为以及与其它 Mesh 路由器节点间的通信行为,并利用多维观测数据训练 HsMM 模型与检测异常。

4.2　HsMM 模型训练

在仿真过程开始时,伴随着大量节点发现、路由发现等过程,整个网络还未进入平稳运行的状态。由于需要描述的是网络在正常平稳状态下的运行特征,因此,放弃最开始一段时间内的观测值。取时间段 1000s～4000s 内观测序列,取样间隔为 1s,每 1000s 内观测值单独作为一个序列,则共有 90 个多维观测序列形成模型训练集 Train dataset。取时间段 4000s～7000s 时间段内观测序列作为模型测试集 Test dataset,每 1200s 内观测值作为单独一个序列,每个观测序列有 1200 个观测值,共 90 个观测序列形成测试集 Test dataset。利用训练集估计 HsMM 模型参数 $\lambda_{train}=(A,P,B,\pi)$,利用测试集评估 HsMM 模型 λ_{train} 描述网络正常运行状态的有效性并进一步调整模型参数。

在用 Train dataset 中的观测序列对模型进行训练以后,可以用该模型实时地对每一个观测序列进行"正常"性测量,即计算观测序列相对于给定 HsMM 模型的熵:$\ln(\Pr[\vec{o}_t^T|\lambda])/t$,其中,$t$ 是观测序列的长度,随着时间的推移而增长。图 3 所示为训练集/测试数据集中观测序列相对于 HsMM 模型 λ_{train} 的熵随序列长度的变化曲线。图 3(a)对应训练集中观测序列。可以看出,随着观测序列的增长,其"正常"性趋于一个定值,各观测序列的"正常"性都落在一个狭长的区间内(在−5 至−4.5 之间)。为评价 HsMM 模型对网络正常行为状态的描述情况,我们计算测试集中观测序列对 HsMM 模型 λ_{train} 的熵,如图 3(b)所示。可以看出,各测试观测序列的"正常"性也都落在同样的区间。



(a) Train dataset　　(b) Test dataset

图 3　训练集/测试数据集对 HsMM 的熵随序列长度的变化曲线

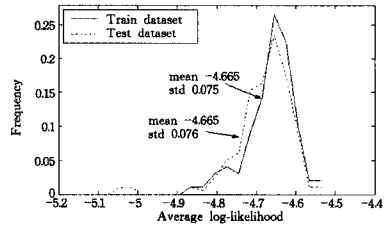


图 4　训练与测试集观测序列对模型的熵分布

图 4 所示为训练集与测试集观测序列对检测模型的熵分布。经过高斯拟合,训练集观测序列的熵服从($mean=$

$-4.665, std=0.075$)的正态分布，测试集观测序列的熵服从($mean=-4.665, std=0.076$)的正态分布。可见，HsMM 模型能对网络正常行为状态进行有效描述。对于测试集，当取阈值 $\delta=-5$ 时，只有 2 个观测序列相对 HsMM 模型 λ_{train} 的熵小于 δ，即正常观测序列被误判为异常的概率为 2.2%。

4.3 恶意攻击检测

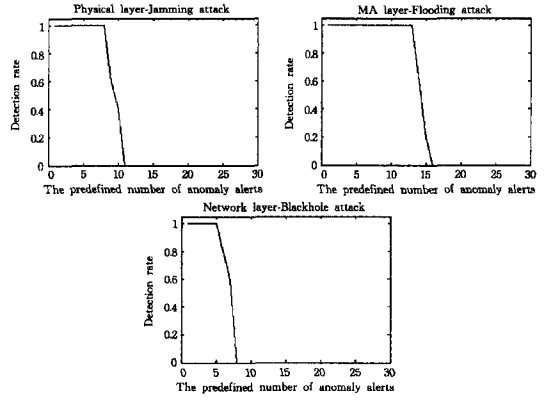
为进一步评价 HsMM 对网络恶意攻击的检测能力，本文仿真利用一个恶意 Mesh 路由器节点实现几种典型的针对不同协议层的网络攻击，包括物理层 Jamming 攻击、MAC 层泛洪攻击以及网络层黑洞攻击。对每种攻击，我们进行 5 次仿真实验，每次恶意 Mesh 路由器节点发起恶意攻击的位置不同。

每个运行 IDS 的 Mesh 路由器节点采集观测序列，并计算其“正常性”。如果观测序列相对于给定 HsMM 正常模型的熵大于某个阈值 δ，即 $\ln(\Pr[\vec{o}_1^t|\lambda])/t>\delta$，则认为发现本地异常，根据正常情况下观测序列对 HsMM 模型的熵分布，本文实验先取 $\delta=-5$。在本文中，预定义 n 值，如果 n 个($1\leqslant n\leqslant N$，N 为全部 Mesh 路由器节点数量) Mesh 路由器节点联合报告本地异常，则认为存在恶意攻击。

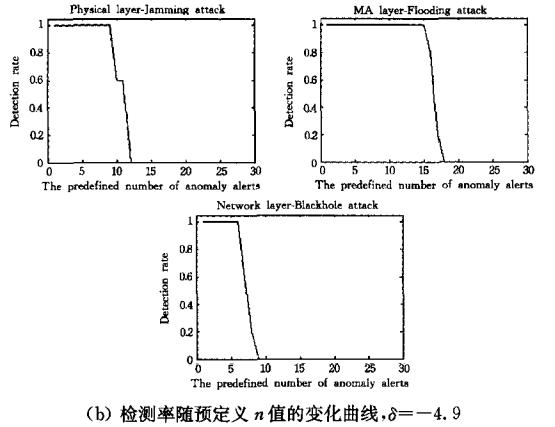
对物理层 Jamming 攻击进行 5 次仿真，如表 4 所列，可见每次仿真中报告异常的节点数量随攻击发起位置有所不同。若取 $n=9$，那么该检测模型对 Jamming 攻击的检测率为 100%。

表 4　5 次 Jamming 攻击检测情况

Jamming Attack simulation scenario	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ
Number of anomaly alerts	9	11	11	9	12



(a) 检测率随预定义 n 值的变化曲线，$\delta=-5$



(b) 检测率随预定义 n 值的变化曲线，$\delta=-4.9$

图 5

对其他两种攻击也分别进行 5 次仿真，各个攻击的检测率变化随预定义 n 值变化的曲线如图 5(a)所示。可以看出，每种恶意攻击都会影响到部分 Mesh 路由器节点，使其观测序列相对正常 HsMM 模型 λ_{train} 的熵小于阈值 $\delta=-5$。同时，由于无线 Mesh 网网状拓扑的健壮性，恶意攻击影响的范围并没有扩散到全网，每种攻击所导致的异常报警的数量并不相同。就影响范围而言，泛洪攻击最广，而黑洞攻击表现得较为隐蔽。因此，n 值的选取关系到模型对各种恶意攻击的检测效果，当 n 值选取过大时，有可能会漏检某些影响范围小的恶意攻击。以 $\delta=-5$ 为例，若取 $n=3$ 时，那么所仿真的 3 种恶意攻击都能准确检测，且此时误检率仅为 $(0.022)^3$，基本可以忽略。

图 5(b)为 $\delta=-4.9$ 时，检测率随预定义 n 值的变化曲线。可以看出，对同种攻击，异常报警的数量有少量增加，这是由于某些模糊序列被判定为异常。这时，检测模型的误检率会有所提高，为降低误检率，可以适当提高预定义的 n 值。

结束语　本文提出一种无线 Mesh 网络中基于跨层协作的异常检测方法，它采集多协议层结合的多维观测序列来评估其“正常性”，可有效地检测来自于不同协议层的恶意攻击，解决了已有异常检测方法检测能力单一的问题。首先采用 HsMM 模型对 Mesh 网络正常运行状态进行描述建模，即利用正常环境下观测序列训练正常 HsMM 模型，通过计算待评估观测序列对正常 HsMM 模型的熵来评价其“正常性”。进一步，为减小多维度观测序列带来的计算复杂度，本文利用主成分分析方法对观测序列进行降维。通过实验仿真证明，本文方法能有效检测源自于各个协议层的多种恶意攻击行为，包括物理层 Jamming 攻击、MAC 层泛洪攻击以及网络层黑洞攻击，具有一定的通用性。

参 考 文 献

[1] Zhang Y, Fang Y. ARSA: An attack-resilient security architecture for multihop wireless mesh networks[J]. IEEE J. Select. Areas Communications, 2006, 24(10): 1916-1928

[2] Wang X, Wong J, Zhang W. A heterogeneity aware framework for group key management in wireless mesh networks[C]// SecureComm'08. Istanbul, Turkey, September 2008

[3] Prathapani A, Santhanam L, Agrawal D P, et al. Intelligent honeypot agent for blackhole attack detection in Wireless Mesh Networks[C]// IEEE 6th International Conference on Mobile Adhoc and Sensor Systems. 2009: 753-758

[4] Ming Y, Zhou M C, Su W. A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments [J]. IEEE Transactions on Vehicular Technology, 2009, 58(1): 449-460

[5] Yan Y, Cao J N, Li Z. Stochastic Security Performance of Active Cache Based Defense against DoS Attacks in Wireless Mesh Network[C]// Second International Conference on Advances in Mesh Networks. 2009: 30- 36

[6] Bose S, Bharathimurugan S, Kannan A. Multi-Layer Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks[C]// IEEE-ICSCN 2007. MIT Campus, Anna University, Chennai, India, Feb. 2007: 360-365

[7] Bose S, Kannan A. Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks[C]// International Conference on Signal Processing, Communications and Networking. 2008: 182-188

(下转第 110 页)

valued Decision Diagram-based Approach for Multistage System Sencitivity Analysis[J]. IEEE Transactions on Reliability, 2010, 59(3): 581-592

[9] 孙艳蕊，张祥德. 利用极小割计算随机流网络可靠度的一种算法[J]. 系统工程学报，2010，25(2)：284-288

[10] 李振，孙新利，姬国勋. 计算多状态网络可靠度的不交化改进算法[J]. 通信学报，2011，21(9A)：166-172

[11] 王芳，侯朝祯. 用蒙特卡罗和 Petri 网方法估计随机流网络的可靠性[J]. 北京理工大学学报，2004，24(7)：604-608

[12] Liu W, Liu Y, Gu X Q, et al. Monte-carlo Simulation for the Reliability Analysis of Multi-status Network System based on Breadth First Search[C]// 2009 Second International Conference on Information and Computing Science. 2009: 280-283

[13] 刘玲艳，吴晓平，田树新. 基于粗糙集和 Petri 网的随机流网络可靠性评价方法[J]. 控制与决策，2010，25(8)：1273-1276

[14] Hudson J C, Kapur K C. Reliability Bounds for Multistate System with Multistate Components[J]. Operation Research, 1985, 33(1): 153-160

[15] Satitsatain S, Kapur K C. An Algorithm for Multistate Network Reliability Bounds and Its Application[C]// ICQR2005. 2005: 409-417

[16] Satitsation S, Kapur K C. An Algorithm for Lower Reliability Bounds of Multistate Two-terminal Networks[J]. IEEE Transactions on Reliability, 2006, 55(2): 199-206

[17] Prekopa A, Vizvari B, Regos G, et al. Bounding the Probability of the Union of Events by the Use of Aggregation and Disaggregation in Linear Programs[R]. Rutcor Research Report, RRR-4-2001, 2001

[18] Meng F C. A Note on Two Reliability Lower Bounds for Multistate Systems[J]. Probability in the Engineering and Informational Sciences, 2002, 16(4): 485-498

[19] Claudio C, Rocco S, Marco M. Approximate Multi-State Reliability Expressions Using A New Machine Learning Technique [J]. Reliability Engineering and System Safety, 2005, 89(3): 261-270

[20] Ramirez-Marquez J E, Coit D W, et al. Bounds for Multistate Network Two-terminal Reliability[R]. Rutgers University IE Working Paper, 03-121, 2003

[21] Ramirez-Marquez J E. Innovative Approaches in Multistate Network Reliability Modeling and Computation[D]. New Brunswick: The State University of New Jersey, 2004

[22] Jane C C, Laih Y W. A Dynamic Bounding Algorithm for Approximating Multi-State Two-terminal Reliability[J]. European Journal of Operational Research, 2010, 205(3): 625-637

[23] Chiou S N, Li O K. Reliability Analysis of A Communication Network with Multimode Components[J]. IEEE Journal on Selected Areas in Communications, 1986, 4(7): 1156-1161

[24] Yang C L, Kubat P. Efficient Computation of Most Probable States for Communication Networks with Multimode Components[J]. IEEE Transactions on Communications, 1989, 37(5): 535-538

[25] Gaebler R F, Chen R J. An Efficient Algorithm for Enumerating States of a System with Multimode Unreliable Components[R]. U. S. Sprint Communications, Overland Park, Kansas, Technical Report, 1987

[26] Shier D R, Bibelnieks E, Jarvis J P, et al. Algorithms for Approximating the Performance of Multimode Systems[C]// IEEE INFOCOM 90. 1990: 741-748

[27] Shier D R. Network Reliability and Algebraic Structures[M]. Oxford: Clarendon Press, 1991

[28] 宋月. 若干复杂系统的可靠性分析[D]. 西安：西安电子科技大学，2006

[29] 王冰山，宋月，王玉梅. 两端多状态网络可靠度的研究[J]. 计算机应用研究，2011，28(5)：1863-1865

(上接第 66 页)

[8] Joseph J F C, Lee B S, Das A. Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(2): 233-245

[9] Thamilarasu G, Sridhar R. Game Theoretic Modeling of Jamming Attacks in Ad hoc Networks[C]// Proceedings of 18th Internatonal Conference on Computer Communications and Networks. 2009: 1-6

[10] Yu S Z, Kobayashi H. An Efficient Forward-Backward Algorithm for an Explicit Duration Hidden Markov Model[J]. IEEE Signal Processing Letters, 2003, 10(1): 11-14

[11] Rabiner L R. A tutorial on hidden markov models and selected applications in speech recognition[J]. Proc. of the IEEE, 1989, 77(2): 257-286

[12] Smith L I. A Tutorial on Principal Components Analysis [EB/OL]. http://www.snl.salk.edu/~shlens/pub/notes/pca.pdf, 2003

[13] Yu S Z, Kobayashi H. A Hidden Semi-Markov Model with Missing Data and Multiple Observation Sequences for Mobility Tracking[J]. Signal Processing, 2003, 83(2): 235-250

(上接第 69 页)

[12] Chow S S M, Hui L C K, Siu Ming Yiu, et al. Secure hierarchical identity based signature and its application[C]// Proceedings of ICICS 2004, volume 3269 of LNCS. Springer-Verlag, 2004: 480-494

[13] Au M H, Liu J K, Yuen T H, et al. Efficient hierarchical identity based signature in the standard model[EB/OL]. http://eprint.iacr.org/2007/068

[14] Zhang Le-you, Hu Yu-pu, Wu Qing. New construction of short hierarchical id-based signature in the standard model[J]. Fundamenta Informaticae, 2009, 90(1): 191-201

[15] 李进，张方国，王燕鸣. 两个高效的基于分级身份的签名方案[J]. 电子学报，2007，35(1)：150-152

[16] Ruckert M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles [C]// Proceedings of the 3rd international workshop on PQCrypto 2010, volume 6061 of LNCS. Springer-Verlag, 2010: 182-200

[17] 吴青，张乐友，胡予濮. 标准模型下一种新的基于分级身份的短签名方案[J]. 计算机研究与发展，2011，48(8)：1357-1362