无线自组织网络中多层综合的节点行为异常检测方法

王 涛 余顺争
(中山大学信息科学与技术学院电子与通信工程系 广州 510275)

摘 要 Ad hoc网络由于采用无线信道、有限的电源和带宽、分布式控制等,会比有线网络更易受到入侵攻击。通常的入侵检测技术具有检测能力单一、缺乏对抗新入侵方式的能力等缺陷。在分布式入侵检测系统(IDS)的基础上,提出一种针对移动节点网络行为的异常检测机制。基于多层综合的观测值序列,采用隐半马尔可夫模型(HSMM)建立描述网络中合法节点正常行为的检测模型,继而对网络中的正常与异常行为进行判断与识别。实验表明,此方法能针对现有多种入侵方式进行有效的检测。

关键词 Ad hoc网络,入侵检测系统,异常检测,隐半马尔可夫模型

Multi-layer Integrated Anomaly Detection of Mobile Nodes Behaviors in Mobile Ad Hoc Networks

WANG Tao YU Shun-zheng
(Department of Electronics and Communication Engineering, Sun Yat-Sen University, Guangzhou 510275, China)

Abstract Mobile Ad hoc Networks are very vulnerable to malicious attacks due to the nature of mobile computing environment such as wireless communication channels, limited power and bandwidth, dynamically changing and distributed network topology, etc. The general existing Intrusion Detection Systems (IDS) have provided little evidence that they are applicable to a broader range threats. Based on the generalized and cooperative intrusion detection architecture proposed as the foundation for all intrusion detection, we presented an anomaly detection mechanism to discriminate the illegitimate network behaviors of mobile nodes. By collecting the observation sequences of multiple protocol layers, Hidden semi-Markov Model (HSMM) was explored to describe the network behaviors of legitimate nodes and to implement the anomaly detection for various malicious attacks. We conducted extensive experiments using the ns-2 simulation environment to evaluate and validate our research.

Keywords Mobile ad hoc network, IDS, Anomaly detection, HSMM

1 引言

Ad hoc网络是由一组带有无线收发装置的移动终端组成的一个多跳临时性自治系统。随着Ad hoc网络的应用日益受到重视,国内外对Ad hoc网络安全方面的研究也就越来越深入。现阶段针对Ad hoc的安全研究主要包括以下几个方面[1]:路由安全、密钥管理以及入侵检测等。前两者虽然能够为Ad hoc网络提供一定的安全防护,却无法有效防范来自被俘获主机的攻击,因此入侵检测是安全的第二道保护屏障,在Ad hoc网络中是必需的。Ad hoc网络与固定网络有一些差别,比如Ad hoc网络无固定基础设施;Ad hoc网络的通信链路具有低速率、有限带宽、高误码、电源能量受限等特征,断链在无线传输中非常常见;Ad hoc网络中,某些正常与异常活动没有明显的差别。因此,在有线通信和蜂窝无线通信方面应用的入侵检测系统(IDS)在Ad hoc网络中不再适用,无法达到最优性能。

现阶段对Ad hoc网络上的入侵检测系统主要集中在两个方面:一是对入侵检测系统模型的研究[2,3],此方面受Ad hoc网络特性的影响,主要是在分布式的入侵检测以及联合响应的系统的基础上进行改进,包括基于簇的分层入侵检测结构[4];使用移动代理技术的入侵检测系统[3,5]等等。二是对检测技术的研究[6-9],即误用检测、异常检测等。由于此两种检测技术各有优异,误用检测使用众所周知的攻击模式来匹配和识别已知的入侵,具有检测已知入侵的准确性高和有效性好的优点;异常检测不需要有关入侵的先验知识,具有检测新入侵方式的能力。

在针对检测技术的研究中,大多数是针对Ad hoc网络中的某种具体的攻击手段进行防御,比如电源损耗攻击[10]、拒绝服务攻击[11]等;或者是针对某种具体的路由协议来研究入侵检测方法,比如基于AODV路由协议的入侵检测系统[12]等。另外,现阶段所研究的入侵检测系统大部分采用误用检测的策略,虽然能对某些已知特性的攻击手段进行准确有效的检测,但是对于新的未知的攻击手段缺乏检测能力;或者有些入侵检测系统采用异常检测模型,但提取的观测值以及检

到稿日期:2008-12-11 返修日期:2009-02-25 本文受国家高技术研究发展计划(863计划)专题课题(2007AA01Z449)及国家自然科学基金—广东联合基金重点项目(U0735002)资助。

王 涛(1983—),男,博士研究生,主要研究方向为计算机网络安全,E-mail:wangtaosea@msn.com;余顺争(1958—),男,教授,博士生导师,主要研究方向为网络安全、网络行为分析、网络测量等。

测方法具有局限性，只能有效地检测某种攻击。文献[13]提出了一种多层联合的检测方法，各个协议层各自建立训练不同的检测模型，最后综合各层的检测结果，虽然有较好的检测效果，但在各个协议层分别进行检测很大程度上加重了移动主机的负荷。从上面分析可以看出，现阶段研究的入侵检测方法在应用上都有较大的局限性，系统的通用性差、检测能力单一以及对抗新入侵方式的能力不足。

基于以上现实，本文提出一种与具体的路由协议无关并能检测多种恶意攻击的异常检测机制。我们采集多个协议层的观测值，利用隐半马尔可夫模型(HSMM)[14-16]来描述移动节点网络行为的随机变化过程。首先对提取到的观测值序列进行分析训练与估计，建立描述网络中合法节点正常行为的检测模型，继而对网络中的正常与异常行为进行判断与识别。

2 移动节点网络行为与观测序列选取

节点的位置和移动信息、链路状态信息、路由信息等等都可以作为 Ad hoc 网络入侵检测系统的观测值。但现有的大部分入侵检测通常集中于这些信息的某一方面，从而只能检测出某种特定的入侵方式。为了正确地区分 Ad hoc 网络中正常节点与异常节点，就必须正确描述网络中正常节点的行为。与有线网络不同，无线 Ad hoc 网络中节点行为受到无线网络特性(无线信道、移动性、能源受限等)以及外部环境(地理环境、气候环境等)各方面因素的影响。节点在移动的过程中，始终保持着与周围节点的通信，如向某个目的节点发送数据包、请求通信链路与路由、处理路由更新与请求信息以及更新自身的邻居表、路由信息表等。每个本地节点可观测收集在各个协议层上与周围移动节点通信的数据，在网络正常平稳运行的情况下，这些观测数据则反映周围节点的正常运行状态。但当周围存在异常行为，比如恶意节点通过发送强信号来干扰其他节点的通信，快速的恶意移动导致网络链路的频繁断裂更新而加重网络负担，攻击者发送大量请求数据而消耗无线网络链路带宽等，这些恶意行为在各个协议层的表现与正常情况不同，比如大量的请求数据(如 Arp 请求)则会导致吞吐量降低以及突增的 MAC 层控制数据(如 RTS，CTS 等)。因此，可以利用各个协议层的观测值来建立描述节点正常行为的数学模型。

为了检测发现对 Ad hoc 网络的各种攻击，包括黑洞攻击、重放攻击、路由扰乱攻击、拒绝服务攻击等，需要研究这些攻击的行为特征并选取与之密切相关的观测值。针对物理信道的安全攻击，在入侵检测系统中，可以取接收到的信号强度 RSS(Received Signal Strength)，RTS/CTS 等信号作为观测值，训练建立异常检测模型，加强网络防御检测此类攻击的能力。在现有的针对路由协议攻击中，比较常见的有黑洞攻击、路由扰乱攻击等，针对此类攻击特点，可提取数据包流量信息、路由表的改变信息等作为观测值。针对泛洪攻击、拒绝服务攻击，可以选择数据包流量信息、RTS/CTS 等作为观测值。综合各个协议层的观测值序列，能较全面地表现节点的网络行为。本文将选取接收到的 RTS/CTS、数据包流量信息作为观测值。采集正常通信情况时所有节点的观测值序列，可以训练建立一个通用的描述正常节点网络行为的 HSMM。以每一时刻 t 某一节点收集到相关的观测值组成一个多维的观测值序列，该观测值序列代表了该节点周围能观测的所有节点的行为。同时，观测序列对于给定 HSMM 的或然概率(likelihood)，即反映了周围节点网络行为的正常程度。

3 检测模型结构与算法

3.1 入侵检测系统结构

本文采用分布式的联合入侵检测系统，每个节点都部署有 IDS。节点与周围邻居节点共享本地检测信息并联合发现异常节点。系统结构如图 1 所示。整个系统由数据采集、预处理、检测与入侵响应 4 个模块组成，具体说明如下。

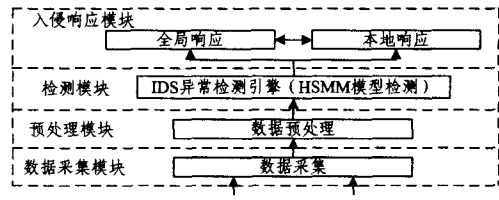

图 1 Ad hoc 网络入侵检测系统结构图

数据采集与预处理模块：主要采集所选取的各个协议层的观测值并进行初步处理，比如量化等，转换成检测模块可以处理的数据格式。

检测模块：检测模块使用异常检测技术，包括本地检测与联合检测两个部分，且都使用 HSMM 来描述节点的网络行为，使用正常情况下的观测数据来训练检测模型。本地节点观测周围节点的各种信息，计算观测值序列对于正常节点网络行为的 HSMM 的或然概率。如果超出某个阈值，则认为周围存在异常节点。同时，本地节点与周围节点交换检测信息，进行联合检测。如果相邻的几个节点都发现有异常行为，则能进一步肯定存在异常节点，从而降低误检率。

入侵响应模块：在发现异常节点后，入侵响应模块根据入侵的类型、网络协议和应用的类型、入侵判定的信任级别等来采取相应的措施。比如，可以重新初始化节点间的通信信道；重新组织网络，以排除已发现的异常节点等。

3.2 HSMM 模型参数训练与异常检测算法

为了更准确地描述节点网络行为，采用多个协议层的观测数据来训练异常检测模型，选取每秒内本地节点接收到 MAC 层的 RTS/CTS 以及网络层数据分组的数量作为观测值。为使各个协议层的观测值同步，取样时间定为 1s。在某个时刻 t，各个协议层的观测值组成一个二维的观测值向量

$$o_t=(RTS_t, Packets_t) \tag{1}$$

RTS_t 是第 t 秒内接收到的 RTS 帧的数量，$Packets_t$ 是第 t 秒内接收到的数据分组的数量。在某一时间段内，本地节点可以得到一个二维的观测值序列。正常情况下，此观测序列代表正常节点的网络行为，并受到各种因素如节点间的相对距离、移动速度、网络活动以及无线网络环境等的影响。我们可以将这些潜在的因素定义为网络的状态，且它们不易被直接观测。对每个给定的状态，由于这些潜在的因素不确定，故对应有不同的观测值向量。因此，可以假定随机过程 $\{o_t\}$ 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状态。HSMM 的隐状态之间的转移关系代表节点及其周围节点的一般移动与通信状态，包括所处位置、移动速率与方向、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 $a_{mn}=\Pr[q_t=n|q_{t-1}=m]$，$m,n\in S$，$q_t$ 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，$p_m(d)=\Pr[\tau_t=d|q_t=m]$，$\tau_t$ 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 $b_m(k)=\Pr[o_t=k|q_t=m]$，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。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[13-15]。针对不同的网络环境，需要对 HSMM 模型参数进行修正。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观测序列对于 HSMM 检测模型的或然概率。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，定义

$$\alpha_t(m,d)=\Pr\{q_t=m,\tau_t=d|o_1^t,\lambda\} \tag{2}$$

其中，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。$\Pr\{q_t=m,\tau_t=d|o_1^t,\lambda\}$ 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

$$\alpha_t^*(m,d)=\Pr\{q_t=m,\tau_t=d,o_1^t|\lambda\} \tag{3}$$

结合上面两式，则有

$$\alpha_t(m,d)=\frac{\alpha_t^*(m,d)}{\Pr\{o_1^t|\lambda\}}=\frac{\alpha_t^*(m,d)}{\sum_{m,d}\alpha_t^*(m,d)} \tag{4}$$

使用 HSMM 前向算法[14,15]来计算或然概率 $\Pr\{o_1^t|\lambda\}$。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

$$\begin{aligned}\alpha_t^*(m',d')&=\sum_{m\in s,d\geqslant 1}\Pr\{q_{t-1}=m,\tau_{t-1}=d,q_t=m',\tau_t=d',o_1^t|\lambda\}\\&=(\alpha_{t-1}^*(m',d'+1)+\sum_{m\in S,m\neq m'}\alpha_{t-1}^*(m,1)a_{mm'})p_{m'}(d')b_{m'}(o_t)\end{aligned} \tag{5}$$

(3)观测序列 o_1^t 对模型 λ 的或然概率为

$$\Pr\{o_1^t|\lambda\}=\sum_{m,d}\alpha_t^*(m,d) \tag{6}$$

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。对于无线移动网，可以有效地节省移动 IDS 主机的存储空间，降低运行负荷，并能及时地发现入侵行为。

4 实验仿真

4.1 仿真实验环境

实验仿真平台为 ns-2，仿真参数设置如表 1 所列。

表 1 仿真参数表

网络参数	数值
拓扑范围	2km×2km
节点移动模式	Random Waypoint Model
节点停留时间	100s
节点数量	100
节点通信距离	300m
节点移动速率	Normal(5,1)
流量数量	20
流量数据速率	4packets/s,512bytes/packet
路由协议	DSR
仿真时间	2h
取样间隔	1s

在仿真过程中，节点移动模式为 RW(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 20 个节点以恒定速率向随机的目的节点发送数据。在仿真过程刚开始时，无线 Ad hoc 网络有大量邻居发现、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，因此取在时间段 1000～3000s 的观测序列作为模型的训练数据集合，共 100 个观测序列，每个观测序列有 2000 个观测值。另外，对 3000～7000s 时间段的观测序列，每 1000s 的时间段作为测试数据集合一个观测值序列，则共有 400 个观测序列，每个序列有 1000 个观测值。利用训练数据集来估计 HSMM 模型参数，并利用测试数据集评估模型参数的有效性和进一步调整模型参数。

图 2 是训练数据集与测试数据集相对模型的对数或然概率分布。除了极少数观测序列对模型的对数或然概率小于 −4.9(占测试集 2%)，大部分序列的对数或然概率大于 −4.9。显然，模型能够很好地描述节点的正常网络行为。如果取或然概率大于 −4.9 为正常观测序列的门限阈值，只有 2%的观测序列被误判为异常序列，即此模型的误检率为 2%。

图 3 是随着测试数据集中观测序列长度的增加序列对模型的对数或然概率的变化曲线图。可以看出，随着序列长度的增加，观测序列的“正常性”趋向于一个定值。另外，可以适当地缩减观测序列的长度，提高异常检测的实时性。

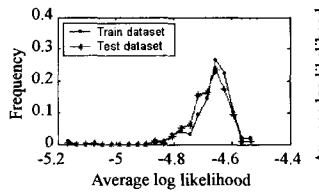

图 2 训练与测试数据集对模型的或然概率分布

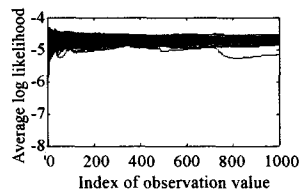

图 3 测试数据集的或然概率随序列长度的变化曲线

4.2 攻击仿真

在 ns-2 仿真实验平台中，本文仿真实现了几种常见的针对 Ad hoc 网络的攻击。在同一网络场景下，让攻击从 500s 的时刻开始，每次攻击持续时间为 5min，并进行多次仿真。

泛洪攻击：本文仿真的两种泛洪攻击方式为单路及多路泛洪攻击。单路的泛洪攻击指某个攻击者向某一目的节点发送大量的伪造数据包或请求。如果目的节点不是邻居节点，则需要经过多跳传送，同时转发节点也成为受害节点。由于网络节点的移动，转发路径也会有改变。多路泛洪攻击指多

个攻击者向单个或多个目的节点发起泛洪攻击。如多个攻击节点将接收到的数据包进行重放，从而形成泛洪攻击；攻击节点短时间内发起大量的 ARP 请求，消耗目的节点通信链路带宽等。

黑洞攻击：攻击节点声称有到某个目的节点的最短路径，在路由更新之后，发往目的节点的数据包都将通过此攻击节点，此攻击节点可随意地篡改或丢弃数据包。

睡眠剥夺攻击：攻击节点选择某个受害节点重放伪造的数据包，或者对外宣称受害节点有到某个目的节点的最优路径，使得受害节点要处理大量的数据，从而不断消耗电源。

4.3 检测结果

本文通过以下两个指标来评价本文异常检测方法的有效性：误检率，指将正常的观测序列判别为异常的数量占所有正常观测序列的比率；检测率，指准确检测出异常攻击的数量占总异常攻击的比率。

图 4 是仿真的某次单路泛洪攻击观测数据集的或然概率分布。可以看出部分节点受到泛洪攻击的影响。采集的观测序列对于检测模型的或然概率小于 −4.9，若阈值取 log-likelihood$<T(T=-4.9)$，则已检测到异常。表 2 为取阈值 $T=-4.9$ 与移动节点停留时间为 100s 时，本文方法对几种网络攻击进行检测的结果。

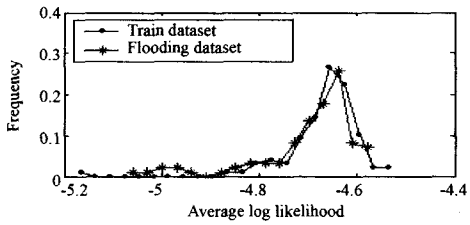

图 4　泛洪攻击观测数据集的或然概率分布

表 2　3 种网络攻击的检测结果

攻击方式	检测率	误检率
泛洪攻击	99%	2%
黑洞攻击	95.5%	2%
睡眠剥夺攻击	93.5%	2%

本文还研究了不同的移动场景对检测模型有效性的影响。基于 RW 移动模型，改变节点移动时的停留时间，依次为 10s，50s，100s，150s，200s 5 个场景。另外，阈值 T 对异常攻击的检测率也有影响。由图 5、图 6 可看出，随着节点移动时停留时间变长，移动网络的拓扑变化趋于缓和，检测模型的误检率降低，检测率上升。总体来说，在各个移动场景下，本文提出的方法能较好地检测泛洪攻击、黑洞攻击与剥夺睡眠攻击，同时维持较低的误检率。

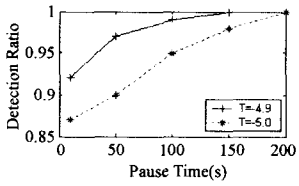

图 5　不同移动场景下针对泛洪攻击的检测率

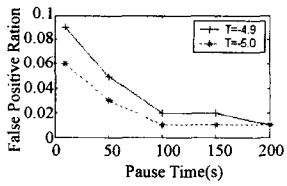

图 6　不同移动场景下检测模型的误检率

结束语　本文提出了一种针对移动节点网络行为的异常检测方法：基于多个协议层的观测序列，利用 HSMM 建立描述移动节点正常网络行为的检测模型。经过仿真实验验证，本方法能对多种攻击进行较好的检测，有效地解决了当前检测方法检测能力单一的问题，并能检测到新的异常攻击行为，且与无线自组织网络使用的路由协议无关。但本方法还存在一些不足，需要进行更深入地研究，如更科学地选取检测模型的阈值，进一步提高检测模型的实时性；评估模型针对其他多种攻击方式进行检测的有效性；对发起异常攻击的源节点进行回溯定位等。

参 考 文 献

[1] Zhang Y, Lee W, Huang Y A. Intrusion Detection Techniques for Wireless Ad Hoc Networks[J]. ACM/Kluwer Wireless Networks Journal, 2003, 9(5): 545-556

[2] Puttini R S, Percher J-M, Mé L, et al. A Modular Architecture for a Distributed IDS for Mobile Ad Hoc Networks[C]// Lecture Notes on Computer Science. vol. 2669, Springer-Verlag, 2003: 91-113

[3] Jansen W. Intrusion Detection with Mobile Agents[J]. Computer Communications, Special Issue on Intrusion Detection, 2002, 25(15): 1392-1401

[4] Vassilaras S, Vogiatzis D, Yovanof G S. Security and Cooperation in Clustered Mobile Ad-hoc Networks with Centralized Supervision[J]. IEEE Journal on Selected Areas in Communications, Special Issue on Network Security, 2006, 24(2): 329-342

[5] Puttini R, Percher J-M, Mc L, et al. A Fully Distributed IDS for MANET[C]// Proceedings of the 9th IEEE Symposium on Computers and Communications (ISCC'2004). 2004: 331-338

[6] Liu Yu, Li Yang, Man Hong. MAC Layer Anomaly Detection in Ad Hoc Networks[C]// Proceedings of the 6th IEEE Information Assurance Workshop. June 2005: 402-409

[7] Sun B, Wu K, Pooch U. Routing Anomaly Detection in Mobile Ad Hoc Networks[C]// 12th Int'l Conf. on Computer communications and Networks (ICCCN'03). Dallas, TX, Oct. 2003: 25-31

[8] Novikov D, Yampolskiy R V, Reznik L. Anomaly Detection Based Intrusion Detection[C]// Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06). April 2006: 420-425

[9] Anjum F, Subhadrabandhu D, Sarkar S. Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols[C]// IEEE 58th Vehicular Technology Conference, vol. 3. IEEE Press, 2003: 2152-2156

[10] Nash D C, Martin T L, Ha D S, et al. Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices[C]// IEEE Int'l Conf. on Pervasive Computing and Communications Workshops. 2005: 141-145

[11] Carl G, Kesidis G, Brooks R R, et al. Denial of Service Attack Detection Techniques[J]. IEEE Transactions on Internet Computing, 2006, 10(1): 82- 89

[12] Sun Baolin, Hua Chen, Li Layuan. An Intrusion Detection System for AODV[C]// Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS '05). 2005: 358-365

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

[14] Rabiner L R. A tutorial on hidden Markov models and selected application in speech recognition[J]. Proceedings of the IEEE, 1989, 77(2): 257-286

[15] 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

[16] 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