文章编号:1004-2474(2014)05-0853-04

入侵检测中基于检测点覆盖度的包流量模型

王 骐[1,2],蔡子元[2],范慧璞[2]
(1. 湖北第二师范学院 物理与机电工程学院,湖北 武汉 430205;2. Florida State University,Tallahassee 32310)

摘 要:无线传感器网络入侵检测系统无论采用哪种框架模型和算法,对其性能评估都需借助于模拟的实验平台。在这个模拟的实验平台中,数据流量模型成为评估入侵检测系统性能客观而全面的重要因素。根据监测区域内目标检测点的覆盖度,提出了一种适用于无线传感器网络入侵检测应用的包流量模型,并通过仿真对理论分析进行了验证。仿真和实际应用表明,该流量模型为无线传感器网络的流量构建了一种数据源模型,根据实际流量负载对无线传感器网络的入侵检测系统的性能进行评估,不仅精确度较高,且易于分析。

关键词:无线传感器网络;入侵检测;检测点;覆盖度;包流量模型;仿真
中图分类号:TN911.1;TP391.9 **文献标识码**:A

Packet Traffic Model Based on Coverage Degree of Sensed Points in Wireless Sensor Networks Intrusion Detection

WANG Qi[1,2],CAI Ziyuan[2],FAN Huipu[2]
(1. College of Physics and Electromechanical Engineering,Hubei University of Education,Wuhan 430205,China;
2. Florida State University,Tallahassee 32310,USA)

Abstract: The performance assessment is required using simulation experiment platform no matter what kind of frame model and algorithm is utilized in wireless sensor network intrusion detection system, in which the packer traffic model is an important factor for assessing the performance of intrusion detection systems objectively and comprehensively. According to coverage degree of the sensed points within the surveillance area,a packet traffic model was proposed, which could be applied to wireless sensor network intrusion detection system by means of the simulation tool. The theoretical analysis was verified. Simulation results and practical application showed that the proposed packet traffic model built a data source model for the data traffic of wireless sensor network, according to the actual traffic load; it could assess the performance of wireless sensor network intrusion detection system with high accuracy and easy to analysis.

Key words: wireless sensor network; intrusion detection; sensed points; coverage degree; packet traffic model; simulation

0 引言

随着无线传感器网络入侵检测系统研究工作的不断发展,采用不同框架模型和算法的入侵检测系统越来越多样化。无论采用哪种框架模型和算法,实际的评估操作都离不开模拟的实验平台,在这个模拟实验平台中,包流量的产生成为入侵检测系统评估结果客观全面的重要因数。为无线传感器网络的流量构建精确而易于分析的源模型,除可根据实际流量负载对无线传感器网络的性能进行评估,还将对网络协议的进一步研究奠定基础。目前普遍采用的包流量模型可分为恒定比特率(CBR)的数据流量模型[1]及可变比特率(VBR)的数据流量模型。文献[2]中的泊松分布包流量模型是以这种数据量模型作为数据源。实际上,流量模型的形成由实际应用决定,可分成实际驱动型和周期生成型。在事件驱动型的应用场景中,如目标检测和追踪产生的流量具有突发性,既不能看成是CBR模型,也不能看成是一种泊松分布的VBR模型。因此,在研究流量模型时,需预先定义实际应用中的参数(如节点密度、目标的移动速率等)。本文介绍了一种基于无线传感器网络入侵检测的包流量模型,针对网格结构的所有条件均不需要。概率覆盖度模型类似于一

收稿日期:2013-11-19
基金项目:2012年湖北省教育厅科研计划基金资助项目(B20123102)
作者简介:王骐(1970-),男,湖北武汉人,副教授,博士,主要从事无线传感器网络安全、嵌入式系统应用的研究。目前在美国Florida State University作访问学者,主要从事无线传感器网络安全的合作研究。

种概率隐式终端模型，它是计算数据包传输概率所采用的包流量模型[3-5]。

1 覆盖度的概念

对于事件驱动型的传感器网络，包流量的产生主要依赖于：

1）事件点的覆盖度，即检测事件点的传感器节点数量。

2）监视区内事件的分布。

由于传感器节点对事件的检测是一种能耗较大的操作，所以检测过程有固定的占空比（如 1%，相当于每秒钟有 10 ms 时间处于检测过程）。

假定 Δt 为检测周期，即在 Δt 内，每个节点检测 1 次。因此，如果目标在时间 t 位置(x,y)处被某节点检测到，那么该目标在时间 $t+\Delta t$ 位置(x',y')处会被同一节点再次检测，点(x,y)和(x',y')之间的欧式距离为 $v\Delta t$，其中 v 为$(t,t+\Delta t)$时间内目标移动的速率，点(x,y)处产生的流量（数据包的数量）等于该点的覆盖度 $c_{x,y}$。

考虑简化，采用二进制数来表示检测结果。如果当目标位于节点的检测范围 R 内，那么目标被检测到的概率为 1，反之则为 0。这样，某点的覆盖度概率与这点的 R 范围内传感器节点数量的概率有关。这是因为，只有与该点相距不大于 R 的节点才能检测到目标。一旦节点部署完毕，那么该节点是否处于某点 R 范围内的事件相当于伯努利试验，成功的概率为

$$p=\frac{\pi R^2}{jk} \tag{1}$$

式中 j,k 分别为监视区域边界的长度和宽度。因此，某点 R 范围内传感器节点的数量形成伯努利分布，监视区域边界示意图如图 1 所示。由于在一般的入侵检测应用中，N 值较大而 p 值较小，这种伯努利分布可近似表示成泊松分布。因此，这种等效的泊松分布的均值为

$$\lambda=Np=\frac{N\pi R^2}{jk} \tag{2}$$

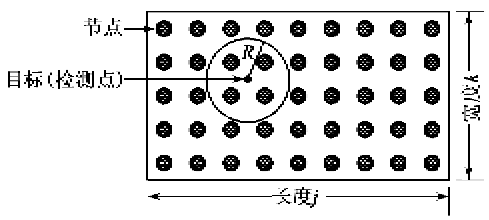
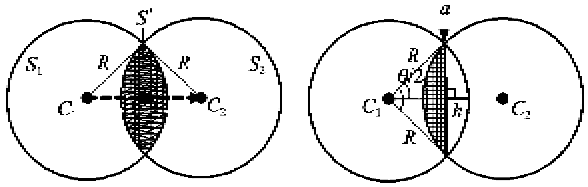


图 1 监视区域边界示意图

2 包流量模型

网络流量模型是一种基于时间的流量模型，监视区域内相邻两点的覆盖度概率并不是相互独立的，而是前后相关，如图 2 所示。C_1 和 C_2 分别为 2 个圆的圆心，假设 C_1 和 C_2 为 2 个连续的目标检测点。由图可看出这种相关性产生的原因。C_1 和 C_2 的间距为 $v\Delta t$。点 C_1 和 C_2 的覆盖度分别为 2 圆内的传感器节点数量，2 个圆的交集 S'表示点 C_1 和 C_2 覆盖度的相关度。这表明监视区域内所有点的覆盖度不能根据泊松分布来建立模型。即如果在时刻 t，检测目标的节点数量已知，由于存在相关性，那么就不能用泊松分布来估计在 $t+\Delta t$ 时刻检测目标的节点数量。为了研究覆盖度的相关性，必须首先分析图 2 中月形面积 S_1、S_2 和交集面积 S'的节点分布概率。



(a) 连续的目标检测的几何图形 (b) 几何图形的参数示意图

图 2 连续目标检测的几何图形

假定随机变量 X_i 表示点 C_i 的覆盖度，Y_i 表示月形面积 S_i 内的节点数量，$i=1,2$，Y'为重叠阴影面积内的节点数量，那么：

$$P(Y'+Y_i=n)=P(X_i=n) \quad (i=1,2) \tag{3}$$

假定点 C_1 的覆盖度为 c_1，即圆内的传感器节点数为 c_1，定义 $c_{\min}=\min(c_1,c_2)$，那么点 C_2 具有覆盖度为 c_2 的概率为

$$P(X_2=c_2)\mid(X_1=c_1)=\sum_{i=0}^{c_{\min}}P(Y'=i)\mid X_1=c_1)\,P(X_2=c_2)\mid Y'=i) \tag{4}$$

已知第 1 个圆内存在的传感器节点数为 c_1，那么其中有 i 个节点存在于 S'内的概率为伯努利分布，其中成功的概率为 $S'/(\pi R^2)$。因此，

$$P(Y'=i)\mid X_1=c_1)=\binom{c_1}{i}\left(\frac{S'}{\pi R^2}\right)^i\left(1-\frac{S'}{\pi R^2}\right)^{c_1-i} \tag{5}$$

另外，有 c_2-i 个传感器节点存在于 A_2 内的概率也为伯努利分布。由于第一个圆内存在的传感器

节点数为 c_1,假定整个监视区域内部署的节点数为 N,那么,整个监视区域除去剪一个圆,余下面积内分布的传感器节点数为 $N-c_1$,因此,

$$P(X_2=c_2\mid Y'=i)=$$

$$P(Y_i=c_2-i)=\binom{N-c_1}{c_2-i}\left(\frac{S_2}{jk-\pi R^2}\right)^{c_2-i}\cdot$$

$$\left(1-\frac{S_2}{jk-\pi R^2}\right)^{N-c_1-(c_2-i)} \tag{6}$$

根据式(4),随时间变化的随机变量 X_t 表示目标位置在时间 t 处的覆盖度,它相当于马尔可夫过程。这个随机变量在不同时刻下的相关度表示为圆的交集,如图 2 所示。根据系统的参数,在任意时刻代表目标位置的圆,可能与前面第 n 个圆相交。那么,这种情况下的马尔可夫过程可看成是剪 n 阶马尔可夫过程,即依赖于前面的 n 个状态,而与后面的状态无关,即

$$nv\Delta t<2R\leqslant(n+1)v\Delta t \tag{7}$$

从而有

$$n=\left\lfloor\frac{2R}{v\Delta t}\right\rfloor \tag{8}$$

式中 $n\in\{0,1,\cdots\}$,以下内容仅考虑 X_t 为一阶马尔可夫过程的情况。

估算基于式(3)～(6)的概率,还需计算出 2 个圆相交的交集面积。由图 2(b)可看出,交集面积 S' 等于阴影部分面积 S''的 2 倍。根据圆的面积与三角函数间的关系,S''可表示[6]为

$$S''=R^2\arccos\left[\frac{R-h}{R}\right]-(R-h)\sqrt{2Rh-h^2} \tag{9}$$

由于存在反余弦函数,式(9)的计算较繁。实际上,文献[7]中给出了计算 S''的近似公式:

$$S''=\frac{2}{3}ah+\frac{h^3}{2a} \tag{10}$$

如图 2(b)所示,θ 为弦 a 的中心角,当 $0°\leqslant\theta\leqslant150°$ 时,式(10)的误差小于 0.1%,当 $150°<\theta\leqslant180°$时,误差小于 0.8%。弦 a 的长度和 h 的高度与 v 和 Δt 有关,即

$$a=2\sqrt{R^2-\left(\frac{v\Delta t}{2}\right)^2} \tag{11}$$

$$h=R-\frac{v\Delta t}{2} \tag{12}$$

根据以上分析,假定在任意点产生的数据包数量等于该点的覆盖度,产生包流量样本的算法流程如图 3 所示。

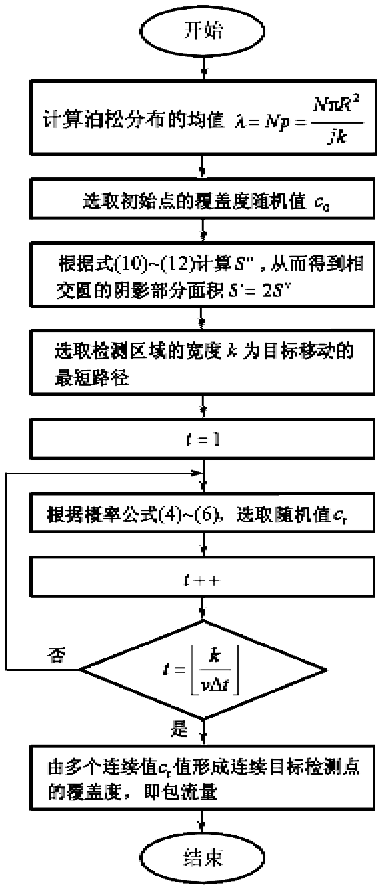


图 3　形成包流量样本的算法流程图

3　仿真结果与分析

在实验场景中,为了研究在传感器节点均匀分布情况下的覆盖度,设定的系统参数值如表 1 所示。如果实验环境中监视区域采用规则的网格,那么监视区域的节点覆盖率至少要达 99%,因此实验中使用的节点数量为 1 000 个。

表 1　实验场景参数值

j/m	k/m	节点数量/个	R/m	v/(m/s)	Δt/s
1 000	1 000	1 000	20	10	1

仿真结果表明,任意点的覆盖度是一个符合泊松分布的随机变量,如图 4 所示。不同色调线代表 1 000 种不同均匀分布的节点部署情况,在每种部署中采集了任意 100 个检测点的覆盖度。图 5 是覆盖度为 2 的点的相邻点的覆盖度柱状图。由图可看出相邻点覆盖度概率的相关性。相邻点是目标的下一个可能的检测点,根据表 1 目标移动速率 v 和检测间隔 Δt 可知,这些相邻点间的间距 $v\Delta t=10$ m。选定覆盖度为 2 的检测点,根据式(4)～(6),其相邻点的覆盖度如图 5 所示,图中将仿真结果分别与理

论分析计算结果、泊松分布情况进行对比。由图 5 可看出，理论分析结果与仿真结果很接近，而与泊松分布差别较大。这也说明，尽管任意点的覆盖度是一个符合泊松分布的随机变量，但相邻检测点的覆盖度并不呈连续泊松分布。

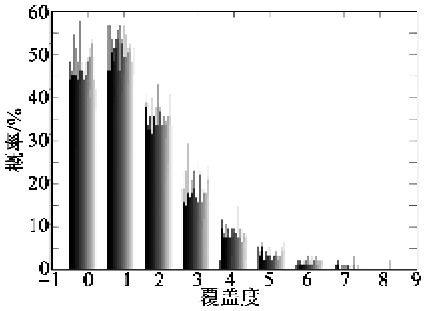


图 4 覆盖度柱状图

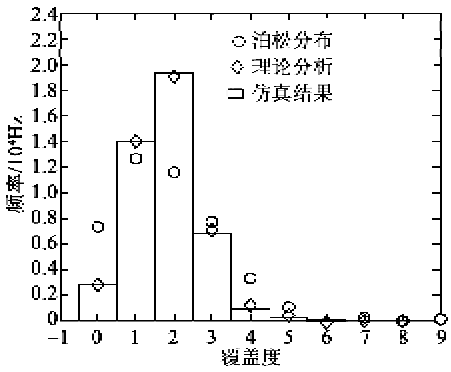


图 5 覆盖度为 2 的点的相邻点的覆盖度柱状图

根据以上分析可知，依据覆盖度的理论计算，可为随后的连续目标检测点建立覆盖度模型，这也是基于无线传感器网络入侵检测的流量模型。

4 结束语

本文设计了一种应用于入侵检测的包流量模型。模型中设计的系统参数包括传感器节点的数量、监视区域大小、检测范围、目标移动速率及采样间隔等。在入侵检测系统评估的过程中，可对系统参数进行设置。在流量产生的过程中，由于流量模型是根据相邻检测点的覆盖度建立的，且任意点呈泊松分布，所以模拟流量更接近于真实流量，分析较易。在入侵检测系统评估的实验平台中，这种流量模型以理论分析为基础，精确度较高，能满足评估的需要。

入侵检测系统评估所需网络流量仿真是一项很复杂的工作[8]，本文提出的流量模型还存在需要完善的地方，如若节点任意分布，对流量模型会产生哪些影响，如何改进，如何产生不失一般性的真实网络流量等等，将是今后继续研究的方向。我们将结合入侵检测系统评估的特点，不断改进现有流量产生模型。

参考文献：

[1] MARTYNOV D, ROMAN J, VAIDYA S, et al. Design and implementation of an intrusion detection system for wireless sensor networks[C]//Chicago, IL, USA: Proceedings of the IEEE International Conference on Electro/Information Technology (IEEE EIT), 2007: 507-512.

[2] MA Y, AYLOR J H. System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology[C]//Boston, USA: IEEE Trans Mobile Computing, 2004, 3: 286-294.

[3] 肖敏，柴蓉，杨富平，等. 基于可拓集的入侵检测模型[J]. 重庆邮电大学学报：自然科学版，2010，22(3)：345-349.
XIAO Min, CHAI Rong, YANG Fuping, et al. Intrusion detection model based on extensible set[J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2010, 22(3): 345-349.

[4] LIU F, CHENG X, CHEN D. Insider attacker detection in wireless sensor networks[C]//Anchorage, Alaska, USA: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), 2007: 1937-1945.

[5] 魏旻，王一帆，李玉. 基于 WIA-PA 网络的周界入侵检测系统设计与实现[J]. 重庆邮电大学学报：自然科学版，2013，25(2)：148-153.
WEI Min, WANG Yifan, LI Yu. Design and implementation of perimeter intrusion detection system based on WIA-PA industrial wireless network[J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2013, 25(2): 148-153.

[6] WANG Q, WANG S, MENG Z. Applying an intrusion detection algorithm to wireless sensor networks[C]// Moscow, Russia: Proceedings of the 2nd International Workshop on Knowledge Discovery and Data Mining (WKDD 2009), 2009: 284-287.

[7] PONOMARCHUK Y, SEO D W. Intrusion detection based on traffic analysis in wireless sensor networks [C]//Shanghai, China: Proceedings of the 19th Annual Wireless and Optical Communications Conference (WOCC), 2010, 1-7.

[8] 兰旭辉，熊家军. 流量模型在入侵检测系统评估中的应用研究[J]. 计算机工程与设计，2005，26(2)：291-292.