基于自回归滑动平均的网络数据流量预测模型

周 强[1] 彭 辉[2]
(沈阳大学信息中心 沈阳 110044)[1] (浙江大学计算机学院 杭州 310018)[2]

摘 要 在无线网络中,对入侵攻击的准确和迅速的检测是关系到无线网络安全的重要问题。各种入侵攻击可以由其导致的网络流量的变化来检测。针对网络流量复杂的非线性以及混沌性,结合网络流量的时间序列特性,提出了一种基于自回归滑动平均(ARMA)的网络数据流量预测模型。该模型利用第三方检测系统,不需要耗费网络资源,能够迅速和准确地预测网络流量。采用从16个信道分析器获得的数据流量测量值对模型进行了初始化。仿真实验结果表明,文中提出的模型能够有效地检测网络入侵攻击,提高了整个网络的性能,延长了网络的寿命。

关键词 无线网络,网络攻击,流量预测,自回归滑动平均
中图法分类号 TP319 **文献标识码** A

Research on Network Traffic Prediction Scheme Based on Autoregressive Moving Average

ZHOU Qiang[1] PENG Hui[2]
(Information Center, Shenyang University, Shenyang 110044, China)[1] (School of Computer, Zhejiang University, Hangzhou 310018, China)[2]

Abstract Detecting intrusion attacks accurately and rapidly in wireless networks is one of the most challenging security problems. Various types of intrusion attacks can be detected by the change in traffic flow that they induce. We proposed an intrusion detection system for WIA-PA networks. After modeling and analyzing traffic flow data by time-sequence techniques, we proposed a data traffic prediction model based on autoregressive moving average (ARMA) using the time series data. The model can quickly and precisely predict network traffic. We initialized the model with data traffic measurements taken by a 16-channel analyzer. Test results show that our scheme can effectively detect intrusion attacks, improve the overall network performance, and prolong the network lifetime.

Keywords Wireless network, Network attack, Traffic prediction, Autoregressive moving average

1 引言

WIA-PA无线网络标准[1-3]是一种工业自动化无线网络标准。它是为了满足工业自动化网络的特殊需求而制定的标准。这些特殊需求包括抗干扰、低能耗等。无线网络易于受到某些类型的网络攻击,因为其布局在公开和无保护的环境中。可以采用一些预先配置的安全系统提高无线网络的抗攻击能力。然而,现有的攻击检测系统都主要专注于有线网络。WIA-PA网络与有线网络的差别决定了传统的攻击检测系统不能直接应用于WIA-PA网络[4-6]。WIA-PA标准提供了一些无线网络的保护措施,然而用于攻击检测的框架和系统都还没有被设计出来。任何新的攻击检测系统都应该满足WIA-PA标准的要求。本文的主要目的在于设计一种能够满足WIA-PA标准的无线网络保护结构。

在具有较高安全要求的网络中,采用入侵检测技术是非常必要的。作为WIA-PA系统中的第二层保护,WIA-PA IDS应该和一些预先设置的安全措施一起工作,比如认证系统、加密技术等。它们应该互相作为对方的补充,并且相互兼容。

数据流量广泛应用于无线传感网络(WSN)的入侵检测。文献[7]研究了用于入侵检测的包数据流量模型。文中对均匀分布的传感器阵列定义了检测区域中各点的覆盖的概率密度函数,仿真表明了这种模型的正确性。然而,网络流量与应用密切相关。大多数WSN流量是时间驱动的,因此流量预测模型不能被用来准确检测入侵。针对网络流量的预测的研究,最初主要有基于AR、ARIMA的线性预测模型[1],算法较简单,但其自适应性较差。随着智能算法的不断发展,其良好的非线性映射能力、灵活有效的学习方式在预测领域的应用中表现出较大的优势和潜力,如BP神经网络、径向基函数神经网络等,已应用于网络流量、金融、水文等多种预测领域[2]。但是,神经网络是一种依赖经验的启发式技术,其学习过程采用经验风险最小化原则(ERM),在小样本情况下容易出现过学习现象从而导致泛化能力低下;另外,神经网络算法的复杂性受网络结构复杂性和样本复杂性的影响较大。这些不足使得神经网络在预测中的应用效果不如期望的那样好。

基于WIA-PA的无线工业网络采用一种超帧结构来规划网络的通信,采用TDMA作为其接入技术。这使得通过将信号分为几个不同的时隙能够让几个不同的设备工作于相同

到稿日期:2013-07-29 返修日期:2013-09-01 本文受国家航天局遥感论证中心项目(科工技2012A03A0939)资助。
周 强(1963—),男,硕士,副教授,主要研究方向为计算机网络,E-mail:13940182095@163.com;彭 辉(1980—),女,硕士,副教授,主要研究方向为计算机硬件开发、数据恢复与数字取证、图像处理。

的频率。多个用户能够连续地传输数据，但是每一个用户运用不同的时隙。在本文中我们提出一种新的 WIA-PA 网络中的包数据流量模型。本文采用从 16 个信道分析器得到的数据流量测量值对模型进行初始化。仿真实验结果表明，本文提出的模型能够有效地检测网络入侵的攻击，提高了整个网络的性能，延长了网络的寿命。

2 入侵检测技术及攻击模型

通常会存在两种类型的入侵检测：基于错误使用的入侵检测以及基于不规则使用的入侵检测。基于错误使用的入侵检测将已知的攻击信号和系统攻击进行编码，然后存储于数据库中。一个 IDS 如果发现当前的行为和数据库中的某种攻击信号类似，就会触发报警。基于错误使用的入侵检测技术在检测新型攻击时效率较低，因为其缺乏相应的攻击信息。相反，基于非正常使用的攻击检测技术，首先需要确定系统的正常状态和用户使用的正常行为，然后将当前行为与系统认为的正常行为做比较。如果当前行为偏离了系统所确认的正常行为，IDS 就会触发报警。基于非正常使用的入侵检测能够检测新型攻击，但是，系统的正常行为很难确认。

基于特定标准的入侵检测技术结合了前两种检测技术的优点，因此是一种非常有前途的检测技术。这种检测技术通过人为地确定特定的标准来确认合法的系统行为。基于特定标准的检测技术与基于非正常使用的入侵检测类似，因为这两种方法都是将当前行为和特定行为相比较。然而，基于标准的入侵检测技术人为地确定系统的合法行为，因此能够降低虚警的概率。这种技术的缺点在于确定系统的合法行为非常耗时。因此，在设计入侵检测技术时需要在时间和虚警之间折中。

设计一种能够检测所有攻击的方法是非常困难的。通过分析现有的攻击能够有效地提取攻击的特点。这在建立 IDS 的过程中是一个非常重要的步骤。在这里我们主要介绍两种具有代表性的无线工业网络 IDS 攻击。第一种是路由逻辑破坏行为。在路由协议中，典型的攻击策略包括陷阱、路由更新风暴、虚构以及修改各种不同的路由控制包。所有这些攻击都能够造成 WIA-PA 网络的严重破坏。第二种是流量歪曲。这种攻击包括数据包丢失、破坏以及数据阻塞。按照攻击目的的不同，攻击者可以选择不同的方法来实现对数据包的控制。除了上面讨论的攻击类型之外，还有其它多种类型的攻击。因此构造一种能够抵御所有攻击的网络系统是非常困难的。

3 系统建模与结构

为了描述 WIA-PA 网络，我们假设这种网络能够提供两个互不重叠的区域。由于这是一种无线网络，因此两个区域的覆盖范围允许存在重叠的部分。可以根据信道分析器的监测范围对这种网络进行划分，这使得所有的信道监测器能够相互配合以完成入侵检测的任务。我们的研究主要专注于 WIA-PA 网络。

我们假设 IDS 检测器之间的信息交换不会被任何攻击所阻止，因为无线通信在本质上是不可靠的。我们假设正常行为和入侵行为存在本质差别，因为如果入侵者只发送一两段数据，攻击行为是很难被检测出来的。我们假设现场设备接收数据并在每一个 WIA-PA 超帧循环中发送数据。如果是不同的数据循环，则数据系列就会呈现出正常的分布。

设计出一种对所有攻击都具有抵御能力的 IDS 系统是非常困难的。相反，采用一种增量提升策略是更可行的办法。一个安全协议至少应该包括能够抵御已知攻击的机制。除此之外，还必须提供能够在将来轻易添加新的安全补丁的系统。由于 WIA-PA 网络可接入性非常重要，我们主要专注于如下类型的攻击：拒绝服务（DoS）攻击、问候攻击、陷阱攻击以及黑洞攻击。

由于 WIA-PA 系统受制于能量、带宽、处理能力以及存储能力，我们将 IDS 设计为第三方入侵检测和分析系统，如图 1 所示。

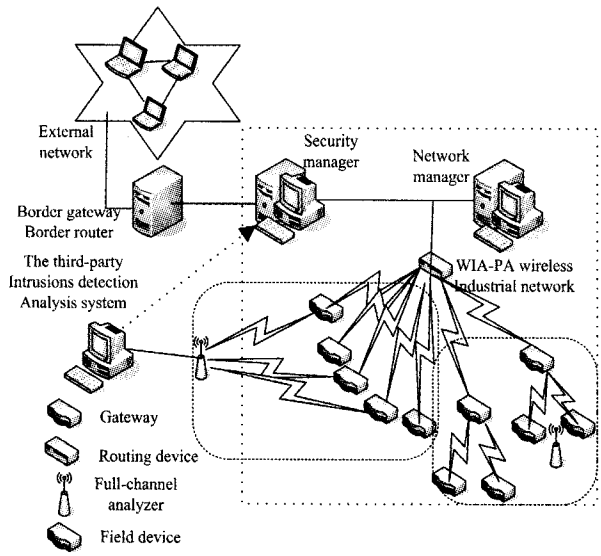


图 1 WIA-PA 网络中入侵检测结构

在传感器网络中的全信道分析器采用轻便的移动监测器来实现实时的数据获取、处理以及集成，从全信道分析器得到的数据可以被收集起来进行分析，然后将结果传送给安全管理器。这会极大地减少整个系统对能量的需求，并且节约带宽。

一个专业的入侵检测分析系统和一个全信道分析器构成了第三方入侵检测系统。全信道分析器能够获取全部 16 条信道 2.4GHz 的网络数据，然后将数据传送给 IDS 专业的入侵检测分析系统，从而轻易地得到分析结果。除此之外，这种第三方入侵检测系统游离于 WIA-PA 网络之外，因此不会消耗网络资源，这在 WIA-PA 这种资源有限的系统中是一个极大的优点。由于这种检测系统的独立性，我们能够在不干扰其它 IDS 操作的同时扩展系统的安全功能。

为了保证实时和可靠的通信，WIA-PA 定义了一种如图 2 所示的超帧结构。

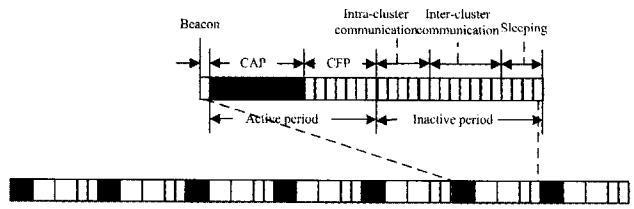


图 2 WIA-PA 超帧结构

WIA-PA 超帧的基本持续时间为 32 个时隙，因为非活动时间段被用作内部数据串通信、外部数据串通信以及休眠。WIA-PA 持续时间定义为 2^N 与基本 WIA-PA 超帧持续时间的乘积。这意味着每一个设备在某一段时间的通信流量是均

匀分布的。因此，我们可以认为所有 WIA-PA 网络流量是一个高频时间序列。这是我们建立模型的基础。

4 网络数据流量预测模型

由于传感器网络的应用数据流量模型具有不平衡特点，因此传感器网络和传统网络不同。首先，由于不平衡的流量模式，越接近路由器的设备其流量负担就越重；其次，大多数应用是需求驱动的，数据流量受到随机需求的影响。一个传感器网络模型必须考虑到以上这些问题。

准确的流量模型能够准确地扑捉到无线网络数据流量的统计特性。本文专注于 WIA-PA 网络的周期数据。考虑到节点能力的有限性，我们采用简单的线性流量分析和预测方法。这种方法的基本思想就是每一个信号都能够表示为前几个样本值的加权和。加权系数由最小周期均方误差决定。

典型的线性预测模型为自回归(AR)和 ARMA。ARMA 模型能够更加有效地分析数据的稳定性。因为 ARMA 预测误差的方差更小，所以它更适合用来做短期预测[8]。

在建立用于预测的 ARMA 模型的过程中，必须从一个稳定的数据序列出发。因此，最初的数据需要预处理。我们采用对数方法减小数据的起伏，使其变得稳定。

(p,q)阶 ARMA 模型是 p 阶 AR 模型和 q 阶 MA 模型的联合体。如果 $q=0$，则模型简化为 AR 模型；如果 $p=0$，则模型简化为 MA 模型。一个时间序列 x_t 服从一个(p,q)阶 ARMA 模型的过程如下：

x_t 是稳态的，且对所有 t 满足：

$$x_t=\mu_t+\phi_1 x_{t-1}+\cdots+\phi_p x_{t-p}+\varepsilon_t+\varphi_1\varepsilon_{t-1}+\cdots+\varphi_q\varepsilon_{t-q}$$

$$\phi_p\neq 0,\varphi_q\neq 0$$

$$E(\varepsilon_t)=0,Var(\varepsilon_t)=\sigma_t^2$$

$$E(\varepsilon_s\varepsilon_t)=0,s\neq 0$$

其中，ϕ_i，φ_i 为模型参数，ε_t 为误差，并且是独立同分布变量[9,10]。

在建立 ARMA 模型时，估计模型参数是至关重要的。主要可以采用统计 F-test、AIC 参数估计准则等方法。在本文中，我们采用自相关函数(ACF)和部分自相关(PACF)方法来估计模型参数。通过分析 ACF 和 PACF 的特点，我们可以确定 ARMA 模型的阶数。

建立准确和易于处理的信源模型是在现有网络协议下的进一步工作的基础。采用实际的数据流对 WIA-PA 网络的性能进行评估。除此之外，系统参数如节点密度以及目标速度等不需要通过仿真来分析。

我们收集了所有信道的 500 个数据流量样本以确定具有代表性的时间序列，采用下面的方法使数据流序列稳定。测量的数据序列可以表示为：

$$X_0',X_1',\cdots,X_i',\cdots,X_n'$$

最初的数据序列如图 3 所示。

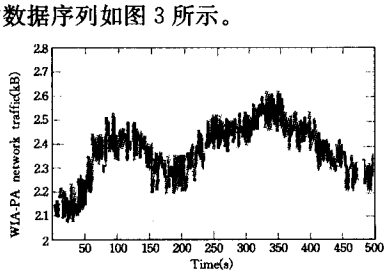


图 3 最初的数据序列

通过对数方法由源数据得到的稳态序列(见图 4)可以表示为：

$$X_0,X_1,\cdots,X_i,\cdots,X_n$$

通过重复上面的步骤，可以将反馈结构从模型中去除。因此，评估输入和输出序列的关系就会变得容易。从输入序列到输出序列的对应关系可以被看作一个转移函数。转移函数的稀疏可以通过最小均方算法进行估计。

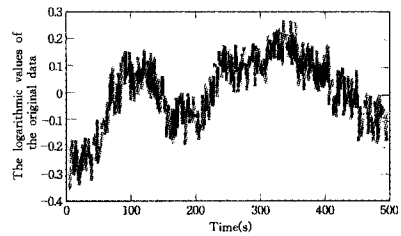


图 4 稳态序列

然后，我们需要确定所得到的时间序列是否是稳定的。为此，我们可以采用 ACF 和 PACF 方法。

ACF 定义为：

$$\rho_k=\frac{\sum_{t=1}^{n-k}(x_t-\bar{x})(x_{t+k}-\bar{x})}{\sum_{t=1}^{n}(x_t-\bar{x})^2} \tag{1}$$

其中：

$$\bar{x}=\sum_{t=1}^{n}x_t/n$$

PACF 定义为：

$$\varphi_{k,k}=\begin{cases}\rho_1, & k=1\\ \dfrac{\rho_k-\sum_{j=1}^{k-1}\varphi_{k-1,j}\rho_{k-j}}{1-\sum_{j=1}^{k-1}\varphi_{k-1,j}\rho_{k-j}}, & k=2,3,\cdots\end{cases} \tag{2}$$

其中，$\varphi_{k,j}=\varphi_{k-1,j}-\varphi_{k,k}\varphi_{k-1,k-j}$。

我们采用 ACF 和 PACF 进行参数估计。对任意 q，我们计算$\rho_{q+1},\rho_{q+2},\cdots,\rho_{q+M}$，其中，

$$M=\sqrt{n}$$

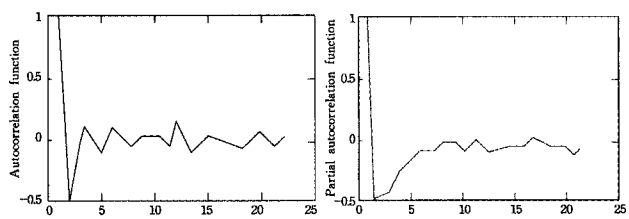
如果 $1\leqslant k\leqslant q_0$，$\rho_k\neq 0$，则$\rho_{q_0+1},\rho_{q_0+2},\cdots,\rho_{q_0+M}\approx 0$。如果满足式(1)的$\rho_k$ 的数量大于 q_0 的 95%，则采用 q_0 作为 ARMA 的系数。

$$\rho_k\leqslant\frac{2\sqrt{(1+2\sum_{n}^{q}\rho_i^2)}}{\sqrt{n}}$$

相似地，对每一个 p，我们计算$\varphi_{k,k}$。如果满足式(2)的$\varphi_{k,k}$的数量大于 p_0 的 95%，则用 p_0 作为 ARMA 模型的系数。

$$\varphi_{k,k}\leqslant\frac{2}{\sqrt{n}}$$

仿真结果如图 5 所示。



(a) 自相关函数 (b) 部分自相关函数

图 5 自相关函数和部分自相关函数

从图 5 中可以看出，利用自相关和部分自相关函数能够很好地用 ARMA 模型描述网络的数据流量。

建模的最后一步就是分析残余误差。通过分析模型的残余误差，能够确认所采用的模型是给定时间序列的一个有效的表述。新的时间序列能够通过预测的最小均方误差获得。我们所得到的数据流量预测模型如图 6 所示。

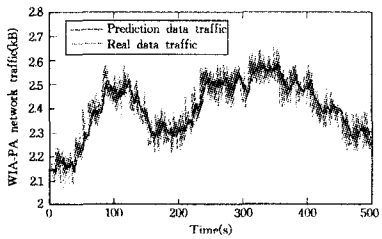


图 6　WIA-PA 数据流量 ARMA 预测结果

基于以上分析，我们采用 ARMA 模型来分析 WIA-PA 网络的数据流量。如果参数 p 太大，则会为实时监测带来沉重的计算压力。因此，我们的算法仅仅采用了 ARMA(1,1) 阶模型。

这样就能够利用 MATLAB 来实施 ARMA (1,1) 阶模型。通过预先采集数据的初始化，就能够将其作为数据流量的预测模型。最终的模型参数为：$\phi_1 = 0.9227$，$\varphi_1 = -0.7885$。其中，$|\phi_1|<1$ 意味着该模型满足稳态时间序列的要求。则我们可以得到如下的表达式：

$$x_t = 0.0227x_{t-1} + \epsilon_t - 0.7885\epsilon_{t-1} = 1$$

5　基于数据流量预测的入侵检测系统

我们采用全信道分析器检测 16 条信道在 2.4GHz 范围内的入侵。由于工业无线网络中全信道通信的特点，全信道分析器将所得到的全网络数据传递到第三方入侵检测系统。在分析整个网络数据流量以后，基于 ARMA 模型的入侵检测分析软件保证系统能够对不同信道的入侵做出迅速和准确的响应。入侵检测系统如图 7 所示。

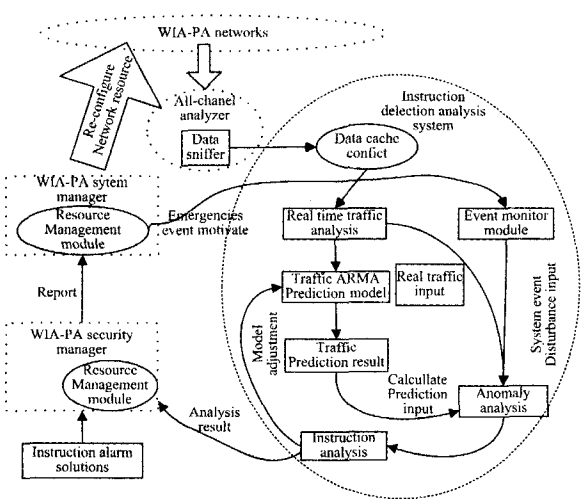


图 7　WIA-PA 网络入侵检测系统

在训练序列期间全信道分析器得到的数据被用作预测模型的输入。实时数据流量也会被传送到异常行为分析模块中。

根据在 $t-1$ 时刻的数据输入，预测模型利用数据流量 x_t 的初始值计算得到的预测数据流量、实时数据流量以及事件噪声将会被异常行为分析模块集中起来。第三方入侵检测系统滤除不必要的和不准确的入侵检测。入侵检测系统随后会分析和比较测量的流量和预测流量。入侵检测分析单元会调整预测模型以使错误预测最小化。在这之后，第三方检测单元会将报告传送给安全管理系统。安全管理系统会根据接收到的第三方检测单元的信息给出报警信息。

安全管理单元会传送一个报告给系统管理单元以告知与入侵相关的情况。同时，利用这些信息，系统管理单元会重新分配系统资源，通过扩展局部入侵检测单元功能和建立经常发生入侵的信道的黑名单，使得尽可能少地利用这些信道传送信息，使得整个系统的安全性得到加强。任意设备都没有必要使协议栈中的入侵检测机制生效，直到 IDS 检测出攻击。一些资源有限的设备没有必要包含这种机制。

安全管理单元会配置 WIA-PA 网络的安全策略，同时根据第三方检测系统的分析结果决定是否使局部入侵检测解决单元生效。

入侵检测解决单元是与安全管理单元和网关集成在一起的。外部入侵检测单元的作用是阻止来自光纤网络的攻击。同时，我们设计了无线网络局部入侵检测单元，以阻止来自无线网络的攻击。

在本文中，我们设定了门限，以将入侵攻击分类。我们采用变化的时间序列来建立数据流量估计模型。同时，我们将测量的数据流量和预测的数据流量相比较，以决定这两者之间的绝对差值是否大于预先设定的门限。在时刻 t，x_t 和 y_t 之间的差值表示为：

$$d_t = x_t - y_t$$

我们采用 RMSE 来衡量模型预测的准确度。如果 $d_t = RMSE > Threshold$，则意味着存在异常流量的情况。

在 WIA-PA 网络中，任何变化都会导致流量的变化，因此我们需要分析造成流量变化的原因。在此我们可以采用基于 WIA-PA 网络中正常噪声水平确定的门限。如果门限设定得较高，则入侵检测率就会变低；如果门限设定得较低，虚警的次数就会增加。在这里，我们根据预先得到的数据选择一个适当的门限。

6　实验分析

本文通过测试来验证基于本文提出的入侵检测系统的 WIA-PA 网络的性能。我们的测试环境包含了 40 个现场设备和 5 个路由器。在安全地将无线网络连接起来以后，无线节点随机地分布在一定的范围内，以收集、处理无线通信数据和完成其它一些任务。现场设备信息通过路由器传送给网关。配置的软件能够实时检测现场设备数据和安全信息。

在联合局部入侵检测单元和第三方入侵检测单元后，我们能够检测并更有效地阻止入侵，因为第三方检测系统能够得到所有网络数据。

测试系统包含了 16 条信道，总共 2.4GHz，从 0×0B 到 0×1A。图 8 所示为得到的实时网络数据。测试结果表明全信道分析器能够捕获网络数据，因此检测分析系统能够分析和比较来自全信道分析器的数据。

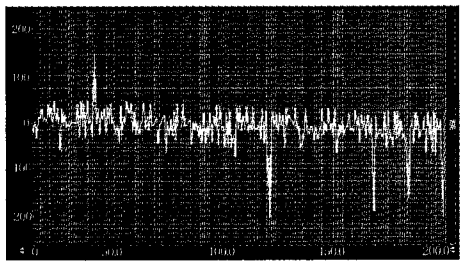


图 8　测试系统的实时流量数据

随后我们在网络中模拟了非法入侵。检测比例和错误率是 IDS 系统的两个重要指标。在我们的系统中检测率和错误率如下所示。

关于检测比例和错误率，我们采用不同的虚警门限，比如将虚警门限设定为最大门限的 0.8、1 和 1.2 倍，以观测因门限不同而导致的性能差异。正如我们所知道的那样，随着门限的升高，检测比例下降。当门限降低时，正常行为的报警信号很容易就超过了门限，从而导致虚警。错误率随着门限的降低而升高。

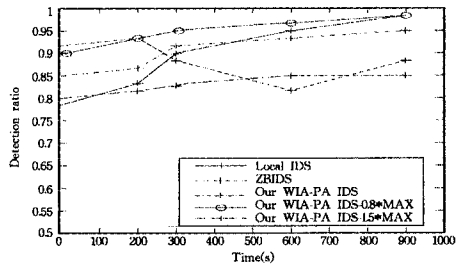


图 9　入侵检测比例

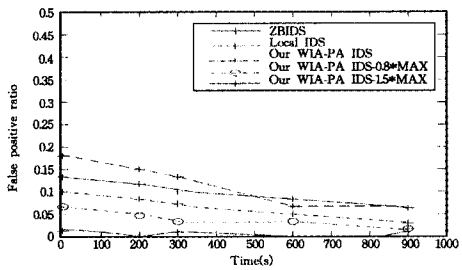


图 10　错误比例

最后，我们将本文方法的检测比例与 ZBIDS[11] 和 LIDS 系统做比较，如图 9 所示。从图中可以看出，我们所提出的系统的检测比例总是大于 90%。和其它系统相比，WIA-PA 入侵检测机制具有很好的检测比例。错误率的仿真结果如图 10 所示。从图中可以看出，WIA-PA 系统的效果比 LIDS 更好，比 ZBIDS 稍差一点，这是完全可以接受的。

结束语　无线工业网络与传统无线网络的区别使得建立安全的无线网络成为一个非常具有挑战性的问题。这些差别包括资源有限的节点、随意布局等。本文提出了一种新的 WIA-PA 网络 IDS 设计方法，该方法采用基于 ARMA 模型的入侵检测方案来提供安全通信的环境。这提供了一种新的安全检测机制。在我们的 IDS 中，采用了能够捕获 16 条信道数据流量的分析器。利用时机的数据流量，我们能够准确和迅速地得到网络流量。测试分析表明这种系统能够保证检测出入侵攻击，提高系统的整体性能，延长网络的寿命，同时能够阻止恶意的数据和不合法的入侵。

参 考 文 献

[1] IEC 62591 Ed. 1. Industrial Communication Networks—Wireless Communication Network and Communication Profiles — Wireless HART [M]. Geneva: International Electrotechnical Commission, 2010

[2] Willig A. Recent and emerging topics in wireless industrial communications: A selection[J]. IEEE Trans. Ind. Informat., 2008, 4: 102-124

[3] Wei M, Zhang X, Ping W, et al. Research and implementation of the security method based on WIA-PA standard[C]// Proc. ICECE. China, Nov. 2010: 1580-1585

[4] Guizani M, Rayes A, Khan B. Network Modeling and Simulation: A Practical Perspective[M]. Chichester, UK: John Wiley & Sons, Ltd, 2010: 260-261

[5] Liu Q, Zhou S, Giannakis G B. Queuing with adaptive modulation and coding over wireless links: Cross-layer analysis and design[J]. IEEE Trans. Wireless Commun., 2005, 4: 1142-1153

[6] 郑黎明，邹鹏，贾焰，等. 网络流量异常检测中分类器的提取与训练方法研究[J]. 计算机学报，2012，35(4)：719-729

[7] Yang T Q. A time series data mining based on ARMA and hopfield model for intrusion detection[C]// Proc. Neural Netw. and Brain. China, Oct. 2005: 1045-1049

[8] 曲桦，马文涛，赵季红，等. 基于最大相关熵准则的网络流量预测[J]. 高技术通讯，2013，23(1)：1-7

[9] 马力，张高明，荀娟迎. 一种基于小波变换的校园网流量预测方法研究[J]. 计算机科学，2012，39(z2)：69-73

[10] 温祥西，孟相如，马志强，等. 小时间尺度网络流量混沌性分析及趋势预测[J]. 电子学报，2012，40(8)：1609-1616

[11] 阎延，郭兴众，魏利胜，等. 采用 RM 算法的 WiNCS 功率控制建模与仿真[J]. 重庆理工大学学报：自然科学版，2013，27(8)：80-84

(上接第 52 页)

[16] Liu Yang-yu, Slotine J-J, Barabási A-L. Control centrality and hierarchical structure in complex networks[J]. Social and Information Networks (cs. SI), 2012, 7(9): e44459

[17] Barabási A-L, Albert R. Emergence of Scaling in Random Networks[J]. Science, 1999, 286(5439): 509-512

[18] den Ouden D-B, Saur D, Mader W. Network modulation during complex syntactic processing[J]. NeuroImage, 2012, 59(1/2): 815-823

[19] Wilting J, Evans T S. Oscillator Synchronization in Complex Networks with Non-uniform Time Delays [J]. Studies in Computational Intelligence, 2013, 476: 93-100

[20] Zhang Lan-hua, Li Yu-juan, Wang Mei, et al. A novel deterministic hybrid complex network model created by innerouter iteration[J]. Nonlinear Dynamics, 2012, 69(4): 1517-1523

[21] Nepusz T, Vicsek T. Controlling edge dynamics incomplex networks[J]. Nature Physics, 2012, 8: 568-573

[22] Yang Xin-song. Stochastic Synchronization of Complex Networks With Nonidentical Nodes Via Hybrid Adaptive and Impulsive Control[J]. IEEE Transactions on Circuits and Systems, 2012, 59(2): 371-384