

基于流量预测的传感器网络拒绝服务攻击检测方案

曹晓梅^{1),2)} 韩志杰³⁾ 陈贵海¹⁾

¹⁾(南京大学计算机软件新技术国家重点实验室 南京 210093)

²⁾(南京邮电大学计算机学院 南京 210003)

³⁾(苏州大学计算机科学与技术系 江苏 苏州 215006)

摘 要 在无线传感器网络中,如何准确和迅速地检测拒绝服务攻击,以保障网络设施的可用性,是一个极具挑战性的安全问题.文中采用线性预测技术,为传感器节点建立了简单高效的 ARMA(2,1)流量预测模型,进而为传感器网络设计了一种基于流量预测的拒绝服务攻击检测方案——TPDD.在该方案中,每个节点独立地完成流量预测和异常检测,无须特殊的硬件支持和节点之间的合作;为了提高方案的检测准确度,提出了一种报警评估机制,减少预测误差或信道误码所带来的误报.模拟实验结果表明,ARMA(2,1)模型具有较高的预测精度,能够实时地预测传感器网络流量;TPDD方案能够在较少的资源开销下,迅速、有效地检测拒绝服务攻击.

关键词 无线传感器网络;入侵检测;线性预测;ARMA模型;拒绝服务攻击

中图法分类号 TP393

DoS Attack Detection Scheme for Sensor Networks Based on Traffic Prediction

CAO Xiao-Mei^{1),2)} HAN Zhi-Jie³⁾ CHEN Gui-Hai¹⁾

¹⁾(National Laboratory of Novel Software Technology, Nanjing University, Nanjing 210093)

²⁾(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003)

³⁾(Department of Computer Science and Technology, Soochow University, Suzhou, Jiangsu 215006)

Abstract In wireless sensor networks, how to accurately and rapidly detect denial of service (DoS) attacks, so as to ensure the availability of network infrastructure, is one of the most challenging security problems. This paper proposes a simple and efficient ARMA(2,1) traffic prediction model for sensor nodes based on linear prediction technique. Then a lightweight DoS attacks detection scheme, TPDD(Traffic Prediction based DoS attack Detection), is designed for wireless sensor networks. In TPDD, each node acts independently when predicting the traffic and detecting anomaly. Neither special hardware nor node's cooperation is needed. Furthermore, a mechanism evaluating reliability of alert is developed to reduce the false alerts caused by prediction or channel error. Simulation results show that ARMA(2,1) model can predict sensor network traffic precisely and swiftly; TPDD is an efficient DoS attacks detection scheme which can quickly detect DoS attacks with less resource overhead.

Keywords wireless sensor networks; intrusion detection; linear prediction; ARMA model; DoS attacks

收稿日期:2007-05-08;修改稿收到日期:2007-07-23. 本课题得到国家“九七三”重点基础研究发展规划项目基金(2006CB303000)、国家自然科学基金(60573131,60673154)、江苏省自然科学基金(BK2005208, BG2007039)以及河南省科技攻关项目基金(072102210044)资助. 曹晓梅,女,1974年生,博士研究生,讲师,主要研究方向为无线传感器网络安全. E-mail: xmcao@dislab.nju.edu.cn. 韩志杰,男,1979年生,博士研究生,主要研究方向为无线传感器网络. 陈贵海,男,1963年生,教授,博士生导师,主要研究领域为并行与分布式计算.

1 引言

无线传感器网络可以实现复杂的大规模环境监测和目标追踪任务,在军事防备、环境监测、交通管理、灾难拯救等众多领域极具应用前景^[1-2].在这些应用中,传感器节点协作地感知、采集和处理网络覆盖的地理区域中感知对象的信息,并以多跳(multi-hop)方式通过无线链路发布给观察者.

传感器网络的无线传输和无人看护等固有特性使它极易受到各种恶意攻击,DoS 攻击是其中对网络可用性危害极大的一类.通常,攻击者通过干扰无线信道,大量重放插入或丢弃报文等手段发起攻击,消耗传感器节点有限的资源,使网络部分或全部瘫痪.因此,当传感器网络被用于具有重要使命的场景中时,如商业上的小区无线防护、军事上的战场监视等等,如何迅速、准确地检测出 DoS 攻击,保证网络设施的基本功能可用,对整个任务的成败至关重要.

传感器网络的资源局限性和应用相关性等特点,决定了对其入侵检测机制的研究是一个极具挑战性的课题,一个行之有效的传感器网络入侵检测系统须要具有简单性、实时性和检测准确性三个特性.目前,已有的传感器网络入侵检测方案^[3-10]大多采用统计分析、隐马尔可夫模型(hidden Markov model)、数据挖掘(data mining)、博弈论(game theory)等方法,通过分析大量的数据或流量特征以及节点间的协同合作判断入侵.这些方案在一定程度上提高了检测结果的准确性,然而实时性较差,难以在攻击发生之后很短的时间内检测出攻击,同时对节点的存储、计算能力提出了较高的要求,额外的通信开销也会迅速消耗节点有限的能量.

为了克服以上方法的缺点,我们为传感器网络设计一种新型的、基于流量预测的 DoS 攻击检测方案——TPDD.它的基本设计思想是从 DoS 攻击会引发网络流量的异常变化这一典型特征入手,分析流量的先后关系,根据已有的流量观测值来预测未来流量,如果真实的流量与其预测流量存在较大偏差,则预示着一种异常或攻击.在本文中,我们首先分析流量预测技术,结合传感器网络资源和流量的特点,为传感器节点建立简单高效的 ARMA(2, 1)模型;随后,设计了一种基于阈值超越的流量异常判断机制,使路径中的节点在攻击发生后自发地检测异常;最后,提出一种报警评估机制,以消除预测误差或信道误码所带来的误报,提高检测质量.分析

和仿真实验结果说明,ARMA(2, 1)模型具有较高的预测精度,能够实时地预测传感器网络流量;TP-DD 方案可以迅速、有效地检测出 DoS 攻击,与同类工作相比,资源开销更小.

2 国内外研究现状

Onat 等^[3]为传感器网络提出一种分布合作式异常检测方案,该方案假定攻击报文具有明显不同于正常报文的能量及速率,每个节点嵌入一个检测引擎,该引擎统计每个邻居节点报文的能量和分组到达速率两种特征值,当发现异常时广播报警信息,如果节点 A 收集的针对节点 B 的报警达到预定阈值,则 A 确定 B 为入侵节点.该方案的局限性有以下两点:首先检测率(detection rate)与攻击者发送报文的能量和速率密切相关,当攻击者采用接近正常值的能量和速率发送报文规避检测时,检测率将大大降低;其次节点合作判断异常引入大量的通信开销,会迅速消耗节点有限的能量和网络有限的带宽,从而缩短网络寿命.Loo 等^[4]给出一种异常检测方案,检测针对 AODV 路由协议的攻击,每个节点配置一个检测引擎,该引擎首先在训练过程中建立正常情况下路由报文流量的特征空间,然后在检测阶段,如果从流经节点的分组中抽取的特征信息出现在特征空间的稀疏区域则判断为发生异常.在该方案中,节点独立地检测异常,从而大大减少了通信开销;然而,由于在训练过程中需要抽取 12 种不同路由控制报文的流量特征,计算每种特征的均值和方差,因此方案的复杂度较高.Rajasegara 等^[5]提出了一种基于数据挖掘的分布式异常检测方案,基站作为树根,父节点定期选举产生.每个叶子节点周期性采集数据流量属性,当一个时间窗截止时,节点对采集到的数据按其相近程度分组,并将分组数据发送给父节点,父节点合并所有子节点的分组并向上一级传递,这个过程反复迭代,直到基站汇总所有分组集合并检测异常,该方案在一定程度上降低集中式执行聚类算法的开销,但实时性较差.借助于在网络中部署少量具有更多资源、能量的高端节点,Doumit 等^[6]提出了基于自组织临界程度(self-organized criticality)和隐马尔可夫模型的入侵检测系统,其中自组织临界程度是一种用于理解复杂系统内部交互的概念,被用于训练隐马尔可夫建模所需的变换矩阵,隐马尔可夫模型被用于预测系统建模.该系统被设计用于异构分簇传感器网络环境,低端节点(簇成员)将采

集到的数据发送给高端节点(簇首),由高端节点实现数据的分析、建模和异常判断. Deng 等^[7]讨论了如何在传递路径中过滤掉伪造和重放的数据包的问题,文章将这一类攻击称为基于路径的 DoS (path-based DoS) 攻击. 在这个方案中,每个节点会生成和维护一个单向 Hash 链表(one-way Hash chain),实现简单的数据源身份鉴别. 单向 Hash 链方式的密钥管理不依赖于公钥加密算法,较适合于传感器节点,但它的密钥链初始化和维护工作较为复杂. Agah 等^[8]将博弈论引入到分簇传感器网络的入侵检测,通过一种只有两个参与者的非零、非合作博弈模型描述攻击者与传感器网络之间的攻防问题,并证明该模型可以达到纳什均衡.

俞波等^[9]提出了一种基于检测点的多跳确认方案(CHECK-point-based Multi-hop Acknowledgement Scheme, CHEMAS),检测选择转发攻击所导致的异常丢包. 该方案中一条传递路径上的部分节点会被随机地选取为检测点,检测点会为它收到的每个事件包生成一个确认包,并将确认包向上游传递,任何传递路径上的中间节点如果没有收到足够的确认包,则会生成异常丢包的警告信息,并经过多跳递交给源节点. 随机选取检测点的方式让敌方无法预知下一次的检测点选择名单,避免了部分节点成为敌方俘获的目标,具有较高的鲁棒性,然而文章仅考虑选择传递攻击,同时确认包的传输和报文的加解密引入了较大的通信和计算开销. 曾鹏等^[10]提出了基于生物免疫原理的传感器网络入侵检测系统,然而文章仅给出了一个概念结构框架,缺乏物理实现和应用.

与同类工作相比,TPDD 在传感器网络 DoS 攻击检测性能上的优势主要体现在以下 4 点:(1) 基于异常检测技术,能够更为有效地检测出传感器网络中形式各异的变种 DoS 攻击;(2) 采用基于线性预测模式生成技术的入侵检测方法,能够更加迅速地检测异常;(3) 采用分布式异常检测策略,每个节点在数据采集的同时独立地完成流量预测和异常检测,既不需要额外的硬件支持,也无须节点之间的合作,资源开销更少;(4) 采用分布式入侵决策和反击策略,在源节点收集报警信息,对入侵作出响应,减少了基地的开销,提高了系统的鲁棒性.

3 传感器节点数据流量模型

3.1 流量模型的选取

准确的流量模型能捕获实际网络流量的统计特

征. 不同于传统网络,传感器网络的流量模式具有不平衡性和应用相关性两个特点:不平衡性体现在传感器网络具有多对一的流量模式,越是靠近基站的节点,流量负担越重;应用相关性体现在:在事件驱动的应用中,以随机突发的数据流为主,在周期性数据查询应用中,对应相对连续、平稳的数据流. 可见,传感器网络流量模型的选取和建立必须与针对的应用场景相关.

Demirkol 等^[11]针对事件驱动应用(如入侵检测)提出了一种覆盖模型,并在此基础上给出了一种传感器网络数据流量模型,同时论证了已有的 Poisson 模型^[12]难以有效地描述传感器网络的流量特征. 本文的研究针对周期性收集数据的传感器网络应用场景. 同时,我们假定网络通过负载均衡技术^[13]实现了流量均衡,防止漏斗效应(funneling effect)导致的网络拥塞.

考虑到节点能力的局限性,我们采用计算简单的线性预测(linear prediction)技术对流量进行分析和预测,它的基本思想是:信号的每个取样值可以用它过去的若干个取样值的加权和来表示;各加权系数的确定原则是使预测误差的均方值最小. 典型的线性预测模型有自回归模型(Autoregressive, AR)和自回归滑动平均模型(Autoregressive Moving Average, ARMA),应用 ARMA 模型能够有效地分析出平稳性数据序列的相关性,比 AR 模型具有更小的预测误差方差,适于进行短期的预测,因此本文采用了 ARMA($2p, 2p-1$)模型对传感器网络的流量进行分析,其中正整数 p 为阶数,如果太大,将产生大的计算量,由于需要做到实时检测,因此在我们的算法中,取常用的 ARMA($2, 1$)模型. 具体建模过程如下.

3.2 平稳化数据序列

假设滑动时间窗的大小为 n ,节点采集到的数据流量序列为 $X'_0, X'_1, \dots, X'_i, \dots, X'_n$, 该序列呈现周期性,但存在一定的非平稳性,为了能够建立 ARMA 模型,需要对 $X'_0, X'_1, \dots, X'_i, \dots, X'_n$ 进行取对数后得到平稳序列 $X_0, X_1, \dots, X_i, \dots, X_n$, 随后用该平稳时间序列建立 ARMA 模型,预测第 $n+1$ 个流量(这样在实时应用中,只要将时间窗口不断往前滑动一次).

3.3 建 模

对处理后的时间序列 $X_0, X_1, \dots, X_i, \dots, X_n$, 建立 ARMA 模型^[14-15], 即

$$\varphi(B)X_i = \theta(B)a_i,$$

其中 B 是后移算子, a_i 是白噪声,它是独立同分布的

高斯随机变量,均值为零,方差为 σ_a^2 . $\varphi(B) = 1 - \varphi_1 B - \varphi_2 B^2$, $\theta(B) = 1 - \theta_1 B$, $\varphi_1, \varphi_2, \theta_1$ 是估计参数. ARMA 相关矩估计方法主要有最小二乘估计方法、最大似然估计方法、最大熵估计方法等等,考虑到传感器节点的计算能力,这里我们采用最小二乘估计方法求解 $\hat{\varphi}_1, \hat{\varphi}_2, \hat{\theta}_1, \hat{\sigma}_a^2$. 随后通过估计参数判断时间序列的稳定性,其稳定性条件为

$$\hat{\varphi}_1 + \hat{\varphi}_2 < 1, \hat{\varphi}_2 - \hat{\varphi}_1 < 1, |\hat{\varphi}_2| < 1.$$

如果满足此条件则视为平稳序列,得出 ARMA 拟合模型如下:

$$X_t = \hat{\varphi}_1 X_{t-1} + \hat{\varphi}_2 X_{t-2} + a_t - \hat{\theta}_1 a_{t-1}.$$

进一步地,我们利用逆函数法进行一步预测, ARMA 的逆函数记为 I_1, I_2, \dots, I_j , 有

$$\begin{cases} I_1 = \hat{\varphi}_1 - \hat{\theta}_1 \\ I_2 = \hat{\varphi}_2 - I_1 \hat{\theta}_1 \\ I_3 = I_j \hat{\theta}_1 \dots (j > 3) \end{cases},$$

则一步预测模型为

$$\hat{X}_t(1) = \sum_{j=1}^m I_j X_{t-j},$$

其中 m 为 X_t 之前 m 次观测值,可根据预测精度的要求取值. 一步预测误差 e_t 为

$$e_t = X_t - \hat{X}_t = - \sum_{j=0}^m I_j X_{t-j}, I_0 = -1.$$

理论和实际结果表明,预测的步数越大,所得的预测值与实际值误差越大^[15],因此为了降低由于预测误差所导致的误警,我们不考虑多步预测.

4 基于流量预测的 DoS 攻击检测方案

4.1 假设

本文提出的检测方案针对具有重要使命的数据收集型传感器网络,网络由大量资源有限的静态传感器节点构成,这些节点定时对被监测对象进行感知,并将所采集的数据发送到基站. 我们假定在传感器节点上已实现链路层、路由层等协议,我们提出的安全协议可以运作在这些协议之上,但并不依赖于具体协议.

WSN 入侵检测系统通常包括检测和响应两个阶段,前者在数据采集传输的同时完成对网络入侵的检测,报警信息将被发送到源节点或者基站;后者指当源节点或基站收集了足够的报警信息后,可以通过运行更为复杂的算法来做出决策并进行反击,例如,可以通知路由协议调整路由、减少可以通过节点的流量,甚至人工检查并移除恶意节点. 本文的研

究着重考虑如何检测出入侵所导致的异常,并不考虑具体的决策与反击措施.

我们假定在部署阶段,传感器网络处于安全状态,每个节点执行定位算法获取自己的位置信息,之后生成节点间共享的认证密钥. 本文直接采用文献[9]中给出的位置绑定 ID 密钥技术,以节点的位置信息作为节点 ID 和双变对称多项式的参数,生成节点间共享密钥,从而在加密和验证的同时,可以根据密钥轻松获得节点位置信息.

TPDD 主要针对对流量有较大影响的 DoS 攻击,如选择转发攻击、hello 洪泛攻击(hello flooding attacks)、污水池攻击(sinkhole attacks)、黑洞攻击(blackhole attacks)等. 对于其他类型的攻击,如编造和篡改数据(spoofed and altered packets)、女巫攻击(sybil attacks)、虫洞攻击(wormhole attacks)等,本文并不考虑相应的防范措施,有兴趣的读者可以参考文献[16].

4.2 异常检测与报警评估机制

在 TPDD 中,每个传感器节点采用 ARMA 的一步预测模型,利用滑动时间窗内累积的数据流量序列估计模型参数,预测即将到达的流量值,之后将得到的真实流量与预测流量比较,判断两者的差值绝对值是否超过了预定的阈值. 设阈值为 T ,时刻 t 的真实流量 X_t 与预测流量 \hat{X}_t 的差值为 $d_t = |X_t - \hat{X}_t|$, 当 $d_t - \epsilon > T$ 时,表明发生流量异常,其中 $\epsilon = E[e_t^2]$ 为预测误差.

在传感器网络中,流量变化可能受多种不定因素的影响,流量异常的原因既可能是由于受到 DoS 攻击,也可能是因为信道误码或网络拥塞,因此如果不区分导致异常的原因而直接报警,将会产生较高的误警. 频繁的误报会导致检测效率降低,影响系统性能,如何减少误报具有重要意义. 本文提出一种简单的报警评估机制,节点根据发现异常的频率确定是否发出报警报文,即只有当节点在指定时间间隔 $\Delta t (\Delta t \geq 0)$ 内检测到 $m (m \geq 1)$ 个异常时,才向源节点发送报警报文. 例如,当 $\Delta t = 0, m = 1$ 时,表示节点在发现异常之后立即向源节点发送报警报文. Δt 和 m 的取值至关重要, Δt 或 m 越大,误判的风险越小,但检测时效性越差. 在具体实现时,可以由管理员根据网络实际的安全情况动态调整设定.

设生成报警报文的节点 ID 为 A ,源节点 ID 为 B ,节点间共享的认证密钥为 K_{AB} ,则报文格式为

$$A \rightarrow B; B \parallel A \parallel \text{MAC}_{K_{AB}}(B, A).$$

报文长度为 8 个字节,其中节点 ID 各 2 个字节,

MAC (Message Authentication Code) 4 个字节. MAC 码的作用是为整个报文生成签名摘要, 防止外部攻击节点伪造、篡改报警报文.

源节点 A 在收到报警报文之后, 验证 MAC 字段判断报文的完整性, 比较通过共享密钥获取的位置信息与节点 ID 是否一致, 丢弃虚假报文. 如果验证结果同时为真, 则启动路由切换机制, 将节点 B 从路径中隔离. 需要指出的有以下两点: 首先在 TPDD 中, 内部攻击者不会伪造虚假报警报文, 其原因在于如果攻击者利用被俘获节点发送报警报文, 结果只能是使被俘获节点自身被隔离, 这种行为对攻击者毫无裨益; 其次, TPDD 利用源节点搜集报警报文,

判断和处理 DoS 攻击, 而不是通过基站, 从而防止了在集中式检测方案中由于“单点失败”所导致的安全瓶颈, 提高了系统的鲁棒性.

5 仿真实验

我们采用 NS2 作为仿真工具, MAC 层协议设定为 802-11, 以 DSR 作为路由协议, 信道误码率为 10%. 实验包括两部分, 首先验证 ARMA 模型一步预测精度, 其次验证当路径中的节点受到不同强度 DoS 攻击时, TPDD 方案的检测准确性以及通信和能量开销. 实验参数如表 1 所示.

表 1 仿真实验参数表

节点数	区域面积/m ²	基站坐标	信道带宽/Kbps	节点初始电能/J	采样周期/s	数据报文大小/B
100	200×200	(0,0)	19.2	2	10	56

5.1 ARMA 模型预测精度仿真

图 1 实线显示路由上的某一传感器节点的网络流量, 利用 ARMA(2,1)模型分析其时间序列, 通过最小二乘法估计出模型参数如下:

$$\begin{aligned}\hat{\varphi}_1 &= 0.86579, \quad \hat{\varphi}_2 = -0.07356, \\ \hat{\theta}_1 &= 0.68954, \quad \hat{\sigma}_a^2 = 0.00186.\end{aligned}$$

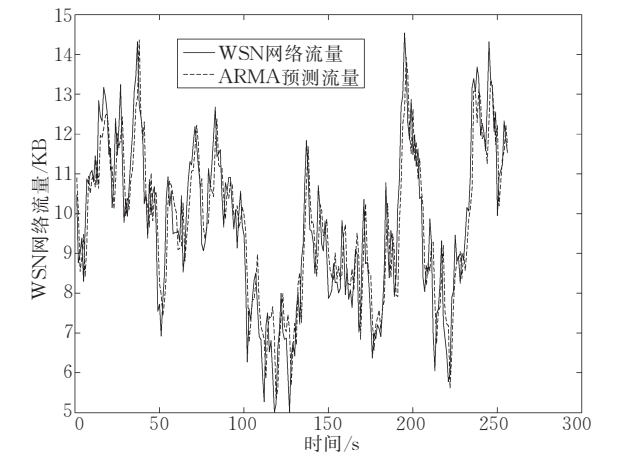


图 1 ARMA 流量预测结果

在这里 $\hat{\varphi}_1 + \hat{\varphi}_2 = 0.79223 < 1$, $\hat{\varphi}_2 - \hat{\varphi}_1 = -0.93935 < 1$, $|\hat{\varphi}_1| < 1$ 满足序列平稳性条件, 可以推出其拟和模型为

$X_t = 0.86579X_{t-1} + 0.07356X_{t-2} + a_t - 0.68954a_{t-1}$. 令 $m=3$, 得到其一步预测模型

$$X_t = \sum_{j=1}^3 I_j X_{t-j}.$$

从任意时刻起在 256s 内, 每秒采样数据流量一次, 利用本模型可计算出其估计值, 其一步预测流量

如图 1 虚线所示. 从图中可以看出, 预测曲线和真实网络流量曲线比较吻合 ($\epsilon \approx 0$), 说明作为一种短时相关预测模型, ARMA(2,1)的一步预测取得了较好的预测效果, 能够作为一种实时网络流量预测模型预测传感器网络流量.

5.2 TPDD 检测性能仿真

在这一节中, 我们通过实验对 TPDD 进行深入的评估, 测试检测准确度、节点的平均能耗和相对通信开销等 3 个性能指标:

(1) 检测准确度. 具体包括检测率和过警率 (false positive rate), 其中检测率表征检测到的恶意报文数量与全部报文数量的比值, 过警率表征检测到的非恶意报文数量与全部检测到的报文数量的比值.

(2) 节点的平均能耗. 分析在正常、有攻击无检测以及有攻击有检测三种情况下节点的平均能量开销.

(3) 相对通信开销. 横向比较在面临相同强度的攻击和信道误码的条件下, 本方案与 CHEMAS^[9]的相对通信开销, 即采用了入侵检测方案后系统总的通信开销与没有采用检测方案的通信开销的比值.

5.2.1 检测准确度

我们在实验中模拟验证当重放报文率从 10%~50% 递增时 TPDD 在不同阈值下的检测率和过警率. 为简化问题, 我们设定 $\epsilon=0$, $\Delta t=0$, $m=1$, 整个实验反复进行了 10 次, 取平均值作为实验结果, 具体如图 2 所示.

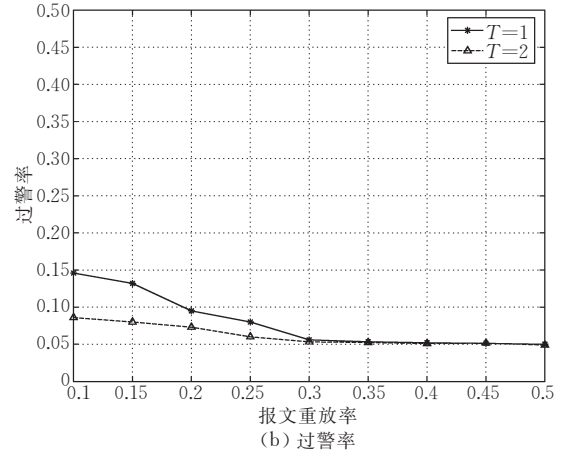
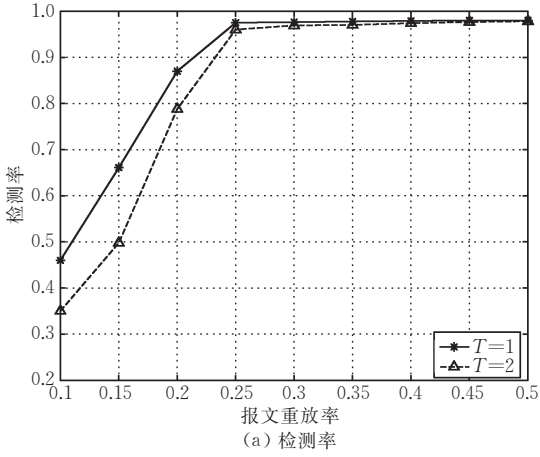


图 2 检测准确度

图 2 所示结果表明:首先,当重放报文率较低时,检测率/过警率与阈值 T 存在密切关系: T 越小,检测率和过警率越高; T 越大,检测率和过警率越低.其次,检测率与重放报文强度存在密切关系:当重放报文率较低时,方案的检测率较低,比如当重放报文率为 10% 时,检测率均低于 50%;然而,当重放报文率超过 25% 之后,不同阈值下的检测率趋同.我们认为产生这种情况的主要原因在于信道误码导致部分报文丢失,致使少量重放报文没有被检测出来,但随着重放报文数量增加,信道误码对检测率的影响越来越小.最后,过警率曲线基本上稳定在一个较低水平,其主要原因是信道误码所导致的丢包在客观上降低了重放报文攻击的过警率.

可见,阈值的设定和攻击的强度决定了攻击的检测结果,其中阈值的设定是关键.为了进一步提高 TPDD 的检测准确性,须要将具体应用场景中的信道误码率以及应用环境的安全需求等因素综合考虑,使阈值 $T, \epsilon, \Delta t, m$ 更加切合应用需求.分析和设定这些参数,识别它们对准确度的影响,设置一种有效的参数设置方法,将是我们后期研究的重点.

5.2.2 节点平均能耗

为了评估系统的平均能量开销,我们分别统计在无攻击、有攻击无检测、有攻击有检测三种条件下节点每传输一个报文的平均能量消耗.我们设定网络中只存在一个攻击者,它可以在任意时刻发起重放攻击,攻击可以持续一个随机长度的时间段.每个节点的初始能量是 2J,我们使用与文献[17]一样的能量消耗模型:使用式(1)计算接收一个报文的能耗,使用式(2)计算发送一个报文的能耗,节点在睡眠状态不消耗能量.

$$E_{Rx} = l \times E_{elec} \quad (1)$$

$$E_{Tx} = l \times E_{elec} + l \times e_{fs} \times d^2 \quad (2)$$

实验结果如图 3 所示.结果表明:当网络中有 DoS 攻击时,节点的能量被大量消耗. TPDD 检测方案能够对检测到的 DoS 攻击做出及时反应,调整网络流量路径,从而将能量消耗限制到一个相对较低的水平.此外,在应用检测机制后,节点处理每个分组的能耗仅增加 0.7mJ 左右,进一步说明了不依赖节点通信合作,而是通过节点独立地预测流量、判断入侵的 TPDD 是一个轻量级的入侵检测方案.

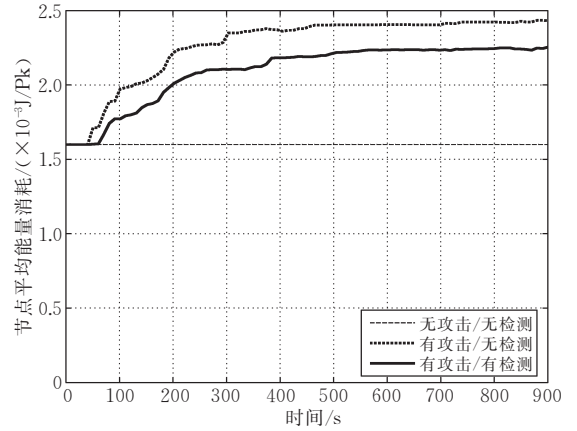


图 3 平均能量消耗

5.2.3 相对通信开销

在这个实验中,我们选择 CHEMAS 作为比较对象,衡量 TPDD 与 CHEMAS 在受到相同强度丢包攻击时的相对通信开销,比较结果如图 4 所示.可见报文丢弃率的大小对通信开销的影响较小.同时, CHEMAS 的相对通信开销较高,约为 1.48 左右, TPDD 的相对通信开销非常小,基本稳定在 1.04 以内.其主要原因在于:CHEMAS 在检测过程中需要路径中检测点交互一定数量的确认报文(11 个字节)和报警报文(12 个字节),而 TPDD 无须节点协

作检测攻击,仅在确认攻击后向源节点发送长度为 8 个字节的报警报文,大大减少了通信开销。

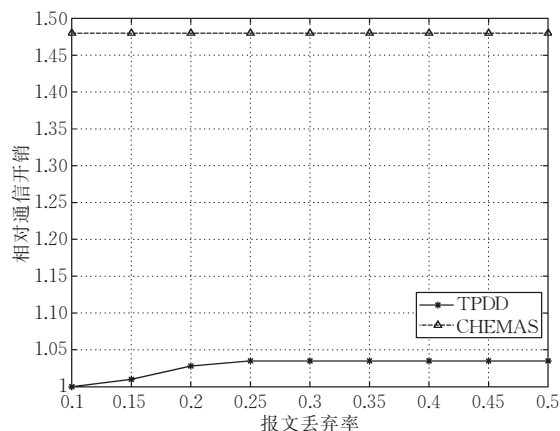


图 4 相对通信开销

6 结 论

本文为数据收集传感器网络提出一种简单有效的 DoS 攻击检测方案. 本文的主要创新点有: (1) 采用 ARMA(2,1), 设计了一种实时的传感器节点数据流量预测模型, 使得计算复杂性降低, 预测精度提高; (2) 将该流量预测模型应用于传感器网络入侵检测系统, 通过流量异常判断和报警评估机制检测 DoS 攻击.

实验结果表明, TPDD 的突出优点是降低了检测过程中的计算和通信开销, 能够实现实时检测, 对突发的较高强度 DoS 攻击具有较高的检测准确度. 然而, 不足之处在于当攻击强度较小时, 受算法预测误差和信道质量等因素影响, 检测准确度下降. 在未来的工作中, 我们将分析和设定这些参数, 识别它们对准确度的影响, 设置一种有效的自适应参数设置方法.

参 考 文 献

- [1] Ren Feng-Yuan, Huang Hai-Ning, Lin Chuang. Wireless sensor networks. *Journal of Software*, 2003, 14(7): 1282-1291(in Chinese)
(任丰源, 黄海宁, 林闯. 无线传感器网络. 软件学报, 2003, 14(7): 1282-1291)
- [2] Sun Li-Min, Li Jian-Zhong, Chen Yu, Zhu Hong-Song. *Wireless Sensor Networks*. Beijing: Tsinghua University Press, 2005(in Chinese)
(孙利民, 李建中, 陈渝, 朱红松. 无线传感器网络. 北京: 清华大学出版社, 2005)
- [3] Onat I, Miri A. An intrusion detection system for wireless sensor networks//*Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB'05)*. Montreal, Canada, 2005: 253-259
- [4] Loo C E, Ng M Y, Leckie C, Palaniswami M. Intrusion detection for routing attacks in sensor networks. *International Journal of Distributed Sensor Networks*, 2006, 2(4): 313-332
- [5] Rajasegarar S, Leckie C, Palaniswami M, Bezdek J C. Distributed anomaly detection in wireless sensor networks//*Proceedings of the 10th IEEE Singapore International Conference on Communication System (ICCS'06)*. Singapore, 2006: 1-5
- [6] Doumit S, Agrawal D P. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks//*Proceedings of the IEEE Military Communications Conference (MILCOM'03)*. Boston, USA, 2003, 22(1): 609-614
- [7] Deng J, Han R, Mishra S. Defending against path-based DoS attacks in wireless sensor networks//*Proceedings of the 3rd ACM on the Security of Ad Hoc and Sensor Networks (SASN'05)*. New York, NY, USA, 2005: 89-96
- [8] Agah A, Das S K, Basu K, Asadi M. Intrusion detection in sensor networks: A non-cooperative game approach//*Proceedings of the 3rd IEEE International Symposium on Network Computing and Application (NCA'04)*. Cambridge, MA, 2004: 343-346
- [9] Yu Bo, Yang Min, Wang Zhi, Gao Chuan-Shan. Identify abnormal packet loss in selective forwarding attacks. *Chinese Journal of Computers*, 2006, 29(9): 1542-1552(in Chinese)
(俞波, 杨珉, 王治, 高传善. 选择传递攻击中的异常丢包检测. 计算机学报, 2006, 29(9): 1542-1552)
- [10] Zeng Peng, Liang Wei, Wang Jun, Yu Hai-Bin. Research on security system of wireless sensor network based on biological immunity principle. *Mini-micro System*, 2005, 26(11): 1907-1910(in Chinese)
(曾鹏, 梁韦, 王军, 于海斌. 一种基于生物免疫原理的无线传感器网络安全体系. 小型微型计算机系统, 2005, 26(11): 1907-1910)
- [11] Demirkol I, Alagoz F, Delic H, Ersoy C. Wireless sensor networks for intrusion detection; packet traffic modeling. *IEEE Communications Letters*, 2006, 10(1): 22-24
- [12] Ma Y, Aylor J H. System lifetime optimization for heterogeneous sensor networks with a hub-spoke topology. *IEEE Transactions on Mobile Computing*, 2004, 3(3): 286-294
- [13] Zhang Chong-Qing, Li Ming-Lu, Wu Min-You. An approach for constructing load-balancing networks for data gathering wireless sensor networks. *Journal of Software*, 2007, 18(5): 1110-1121(in Chinese)
(张重庆, 李明禄, 伍民友. 数据收集传感器网络的负载均衡网络构建方法. 软件学报, 2007, 18(5): 1110-1121)

[14] Zhang Shu-Jing, Qi Li-Xin. Time Series Analysis Concise Guide. Beijing: Tsinghua University Press, 2003 (in Chinese)
(张树京, 齐立心. 时间序列分析简明教程. 北京: 清华大学出版社, 2003)

[15] Zou Bai-Xian, Liu Qiang. ARMA-based traffic prediction and overload detection of network. Journal of Computer Research and Development, 2002, 39(12): 1645-1652(in Chinese)
(邹柏贤, 刘强. 基于 ARMA 模型的网络流量预测. 计算机研

究与发展, 2002, 39(12): 1645-1652)

[16] Karlof C, Wagner D. Secure routing in sensor networks: Attacks and countermeasures. Ad Hoc Networks, 2003, 1(1): 293-315

[17] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Transaction on Wireless Communications, 2002, 1(4): 660-670



CAO Xiao-Mei, born in 1974, Ph. D. candidate. Her current research interests focus on wireless sensor networks.

HAN Zhi-Jie, born in 1979, Ph. D. candidate. His current research interests include time series analysis and P2P computing.

CHEN Gui-Hai, born in 1963, professor, Ph. D. supervisor. His research interests include interconnection networks, high performance computer architecture, graph theory, P2P computing and wireless sensor networks.

Background

The wireless sensor network is a new network technique and typically applied to military, rescue, and digital life environment. The open environment of WSN makes it vulnerable to a wide range of security attacks. Among these attacks, DoS attack is the most destructive one which seriously deplete node resources and damage network availability. Therefore, DoS attack detection scheme should be an indispensable part of WSN, especially for those mission-critical applications.

So far, a few intrusion detection approaches have been proposed for WSN. Almost all of them detect attacks by analyzing large amount of data or traffic features and with node's cooperation. These methods may have higher detection accuracy. However, the complicated calculations and interactive process reduce the efficiency and timeliness of the detection results. To overcome the shortcomings of those methods, the authors propose TPDD, a traffic prediction based DoS attacks detection scheme, which can quickly detect various DoS

attacks with less resource overhead.

This work is supported by the National Basic Research Program(973 Program) of China under grant No. 2006CB303004, the National Natural Science Foundation of China under grants No. 60573131 and No. 60673154, the National Science Foundation of Jiangsu Province under grants No. BK2005208 and No. BG2007039, and the Science-Technology Project of Henan Province of China under grant No. 072102210044. Those projects are conducted around the theories and principles in nowadays network environments, i. e. , wireless sensor networks, Internetwork and P2P systems.

The research team has focused on research of wireless sensor networks for over three years. They have published over 10 papers in highly-ranked international conferences and journals in the fields of security enhancement mechanisms, clustering algorithms and cluster-based routing mechanisms, coverage and topology management, etc.