

无线传感网络的安全访问控制算法研究

聂利颖,王婷婷

(郑州成功财经学院 信息工程系,河南 巩义 451200)

摘 要: 提出一种基于速率变化调整的无线传感网络安全访问控制算法,首先分析无线传感网络访问数据平均输入速率和输出速率、访问数据效率控制、访问数据公平性控制等参数的要求;采用丢包率平滑器,对无线传感网络丢包数据进行平滑处理;最后通过对无线传感网络访问数据包速率变化的调整,实现安全访问控制.实验结果分析证明,利用该算法能够最大限度地利用无线传感网络中的服务资源,实现了无线传感网络的安全访问控制,具有广泛的应用价值.

关键词: 无线传感网络;安全访问;丢包率平滑器;速率变化;控制算法

中图分类号: TP393

文献标识码: A

文章编号: 1000—7180(2017)11—0124—04

Secure Access Control Algorithm for Wireless Sensor Network

NIE Li-ying, WANG Ting-ting

(Department of Information Engineering, Zhengzhou Chengong University of
Finance and Economics, Gongyi 451200, China)

Abstract: This paper proposes a method to match the feature points of user information based on probability generation. In the fusion probability assignment generation theory to set up a user information probability generation model, the latent variables of unknown type defines the user information for the model, calculate the joint probability distribution, distribution of resources of each type of access to a posteriori estimates, given different types of resources associated with the measurement of the threshold, construct the matching feature expression, calculate the most the characteristics of short distance between adjacent types of user information, the user information matching feature points of University library. The simulation results show that the proposed method can improve the accuracy of the feature points matching, which can lay a solid foundation for improving the service quality of University library.

Key words: wireless sensor network; security access; the packet rate smoother; rate of change; control algorithm

1 引言

随着无线传感网络的快速发展,越来越多的用户参与到无线传感网络中,从而造成了越来越多的个人隐私信息暴露于无线传感网络中,用户面临的安全风险也不断增加,用户隐私信息保护问题迫在眉睫^[1-2].近年来,对无线传感网络信息的安全保护成为研究的热点.安全访问控制是对无线传感网络信息资源进行保护的重要手段之一,在用户个人隐私保护过程中具有重要的意义^[3-4].现存的无线传感

网络安全访问控制方法包括自主访问控制和强制访问控制^[5].现存的无线传感网络安全访问控制均为用户主体与客体之间发生的直接关系,对其进行安全管理极其困难^[6].传统的无线传感网络安全访问控制算法采用有效带宽进行无线传感网络的安全访问控制,存在网络服务资源利用率较低的问题^[7].为了保证无线传感网络服务质量,最大限度地利用网络服务资源,缩短安全访问响应时间,业界人士提出了许多很好的算法,在实际应用中起到了一定作用.

文献[8]提出一种基于行为的无线传感网络安

全访问控制算法,该算法存在访问控制安全性不足的问题.文献[9]提出一种无线传感网络安全访问控制算法,利用无线传感网络访问数据包速率抖动实现无线传感网络的安全访问控制.该算法存在安全访问控制效果较差,访问响应时间较长的问题.文献[10]研究了一种利用统计学实现无线传感网络安全访问的控制算法,该算法存在访问控制过程可管理性能较差,服务质量较低的问题.

在上述研究的基础上,针对其在实际应用过程中产生的一系列问题,本文提出一种基于变化速率调整的无线传感网络安全访问控制算法,实验结果分析证明,所提算法提高了无线传感网络访问数据传输服务质量,控制过程可管理性较好,且能够获得较为理想的控制效果.

2 无线传感网络的安全访问控制算法研究

2.1 无线传感网络访问数据拥塞和效率控制

分析无线传感网络访问数据平均输入速率和输出速率、访问数据效率控制、访问数据公平性控制等参数的要求.具体过程如下.

计算无线传感网络访问数据流的最大发送速率,其计算表达式为

$$Q = \frac{\text{size}}{t_{\text{RTT}} \sqrt{\frac{1}{3} p t_{\text{RTO}} \min(1, 3 \sqrt{\frac{3p}{8} p(1+32p^2)}}} \quad (1)$$

式中, t_{RTT} 表示无线传感网络访问数据包传输的往返时间; t_{RTO} 表示无线传感网络访问数据重新传送超时时间; p 表示无线传感网络接收端计算得到的访问数据丢包事件概率; size 表示无线传感网络中访问数据包的大小.无线传感网络访问数据流的最大发送速率 R 的计算,需要先求得无线传感网络访问数据包传输的往返时间 t_{RTT} 、无线传感网络接收端计算得到的访问数据丢包事件概率 p 和无线传感网络中访问数据包的大小 size.

(1) 无线传感网络访问数据包传输的往返时间 t_{RTT}

无线传感网络接收端在反馈访问数据包中包含最近时间内接收到的一个访问数据包的时间戳,反馈给无线传感网络的发送端,则网络发送端依据接收端接收到的反馈访问数据包的时间戳计算出无线传感网络访问数据包传输往返时间 $t_{\text{RTTsample}}$,其计算表达式为

$$t_{\text{RTTsample}} = t_{\text{now}} - t_{\text{timestamp}} \quad (2)$$

式中, t_{now} 表示无线传感网络接收到发送端反馈的访问数据包的时间; $t_{\text{timestamp}}$ 表示无线传感网络接收端反馈访问数据包中包含的时间戳.由于无线传感网络的复杂性,每一个访问数据包的传输周期计算得到的往返时间具有很大的差异性,从而容易造成计算获得的无线传感网络访问数据流最大发送速率产生波动,使得网络发送端由于频繁调整访问数据包发送速率,影响网络整体使用效率.

引用一个带衰变因数的 EWMA 访问数据包过滤器来平滑计算获得无线传感网络访问数据包传输的往返时间,采用小的衰变因数平滑无线传感网络访问数据包传输往返时间,计算公式如下:

$$t_{\text{RTT}} = \alpha * t_{\text{RTTsample}} + (1 - \alpha) t_{\text{timestamp}} \quad (3)$$

式中, t_{RTT} 为式(3)中使用的无线传感网络访问数据包传输的往返时间; α 表示无线传感网络衰变因数,其取值通常在 $[0.1, 0.125]$ 区间; $t_{\text{timestamp}}$ 为式(3)中使用的无线传感网络接收端反馈访问数据包中包含的时间戳.

(2) 无线传感网络访问数据包重新传输超时时间

由于无线传感网络访问数据流在实时多媒体应用中,不允许进行网络访问数据流的重新传输,无线传感网络访问数据重新传送超时时间 t_{RTO} 在实际应用中没有实际意义,只是作为式(1)中的一个参数值参与计算,并不作为无线传感网络安全访问控制的重要访问数据,理论上, t_{RTO} 为无线传感网络访问数据包传输往返时间 t_{RTT} 的 2 倍,在实际应用中表示为 $t_{\text{RTO}} = 4t_{\text{RTT}}$ 参与计算.

(3) 无线传感网络访问数据丢包时间率

在式(1)中使用的是无线传感网络接收端计算得到的访问数据丢包事件概率 p ,为了防止访问数据丢包事件概率出现较大的速率波动,平均丢失间隔需要统计最近几次访问数据包丢失间隔后再进行计算,并且对不同的丢失间隔赋予不同的权重,则无线传感网络访问数据包平均丢失间隔的计算公式如下:

$$l_{(1,n)} = \frac{\sum_{i=1}^n \omega_i l_i}{\sum_{i=1}^n \omega_i} \quad (4)$$

式中, 1 表示无线传感网络访问数据包平均丢失的间隔; l_i 表示无线传感网络中最近第 i 次丢失事件中访问数据包的个数; n 表示无线传感网络的丢包次数; ω_i 表示无线传感网络访问数据包权重.

假设此段时间内的无线传感网络访问数据包个

数足够多,则对平均间隔时间的影响较大,需要考虑这段时间内的无线传感网络访问数据包个数 l_0 . 当无线传感网络访问数据包丢失事件发生时, l_0 转换为 l_1 , l_1 转换为 l_2 ,以此类推可得:

$$l_{(0,n-1)} = \frac{\sum_{i=1}^{n-1} \tau w_{i+1} l_i}{\sum_{i=1}^n \tau w_i} \tag{5}$$

根据上式计算无线传感网络最终使用的丢包事件概率表达式为

$$l = \max(l_{(1,n)} - l_{(0,n-1)}) \tag{6}$$

式中,如果 $l_0 > 2l_{(1,n)}$, 且 $i \geq 1$,说明 l_0 数值过大,而造成无线传感网络访问数据包丢失事件概率的波动,为了减小波动,需要对无线传感网络最近 1 到 n 次丢失事件的权重采用折扣因子进行折扣,即无线传感网络访问数据包的历史折扣,其计算表达式如下:

$$\begin{cases} d_0 = 0, i = 0 \\ d_i = \max(0.5, \frac{2l_{(1,n)}(i \geq 1)}{l_0}), i > 0 \end{cases} \tag{7}$$

根据式(8)对无线传感网络访问数据包进行历史折扣后,访问数据包平均丢失间隔的计算可以转化为以下公式:

$$l = \frac{\sum_{i=0}^{n-1} d_i \tau w_{i+1} l_i}{\sum_{i=1}^n d_{i-1} \tau w_i} \tag{8}$$

通过上述计算,可以得到无线传感网络丢包事件概率 p 为

$$p = 1/l \tag{9}$$

根据式(8)和(9)的计算结果可以求得无线传感网络访问数据流的最大发送速率 Q .

2.2 无线传感网络丢包率平滑器

为了避免无线传感网络服务质量的波动,即无线传感网络访问数据包传输延迟造成的抖动,采用丢包率平滑器,对无线传感网络丢包数据进行平滑处理,其计算表达式为

$$\begin{cases} \rho(m) = (1 - \lambda)\rho(m - 1) + \lambda\rho(m) \\ 0 \leq \lambda \leq 1 \end{cases} \tag{10}$$

式中, $\rho(m)$ 表示在 m 时刻和 $m - 1$ 时刻内的无线传感网络访问数据丢包率; λ 表示无线传感网络访问数据包增加速率;当 λ 减小时,之前计算的无线传感网络访问数据包信息对当前的控制会产生较大的影响;而当 λ 增大时,之前计算的无线传感网络访问数据包信息对当前的控制会产生较小的影响. 根据式(10)可以判断无线传感网络当前的状态是访问过载、轻载,还是正常,为后续无线传感网络的安全访

问控制提供基础.

2.3 基于速率变化调整的安全访问控制算法

依据 2.2 节对无线传感网络状态的分析结果,通过对无线传感网络访问数据包速率变化的调整,实现安全访问控制. 具体步骤描述如下:

假设 $R(m)$ 表示 m 时刻无线传感网络访问数据码流的发送速率, $RateMax$ 表示无线传感网络发送端访问数据最大发送速率; $Ratemin$ 表示无线传感网络发送端访问数据最小发送速率,则:

$$R(m) = \begin{cases} \min\{R(m - 1) + \zeta(1 - \rho(m)), RateMax\} & 0 < \rho(m) < 2\% \\ R(m - 1), 2\% \leq \rho(m) < 4\% \\ \max\{R(m - 1) + \delta\rho(m), Ratemin\} & \rho(m) \geq 4\% \end{cases} \tag{11}$$

式中, ζ 和 δ 表示无线传感网络访问数据速率调整常量,根据无线传感网访问数据包传输速率和当前网络状态分析,需要对这两个常量进行相应调整. 从而实现无线传感网络的安全访问实时控制,提高了无线传感网络访问数据包传输的服务质量.

3 实验结果与分析

实验采用 DiskSim4.0 软件对本文提出的基于速率变化调整的无线传感网络安全访问控制算法的精确性进行验证. 无线传感网络存储系统型号为 D2-310,磁盘阵列配置模式为 RAID1,操作系统为 Windows8,访问数据包通过条纹化均匀散布到每个磁盘上. 无线传感网络存储系统访问数据请求完成比例上限 $p = 1\%$,多媒体应用的服务质量 QoS 需求为 $d = 480$ ms.

分别计算采用文献[8]算法和文献[9]方法与本文提出的方法时,网络存储空间允许的最大并发多媒体应用访问数据数量. 计算中文献[8]算法使用的磁盘服务访问时间和文献[9]算法使用的磁盘服务访问时间,都是由相关生产厂商提供的精确的磁盘参数计算得到,并通过实验测试分析进行一一核对. 表 1 所示为采用不同算法的无线传感网络最大并发应用个数.

表 1 采用不同算法的无线传感网络最大并发应用个数

文献[8]算法	文献[9]算法	本文算法
395	248	387

图 1 为采用文献[9]算法进行安全访问控制的情况. 其中无线传感网络访问数据请求时间都不能大

于 d , 无线传感网络多媒体应用的服务质量 QoS 需求能够得到保障. 但此刻无线传感网络的存储系统服务资源利用率较低, 其完全空闲时间达到了 46.2%.

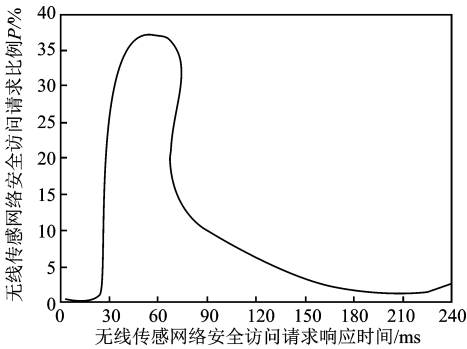


图1 文献[9]算法访问最大并发应用数量为 248 时的响应时间分布曲线

图 2 为采用文献[8]算法进行无线传感网络安全访问控制的情况. 此时无线传感网络大部分访问请求的响应时间均不大于 d , 只有 11% 的无线传感网络访问请求的响应时间小于 480 ms, 明显不能保证无线传感网络中多媒体应用的服务质量 QoS 需求.

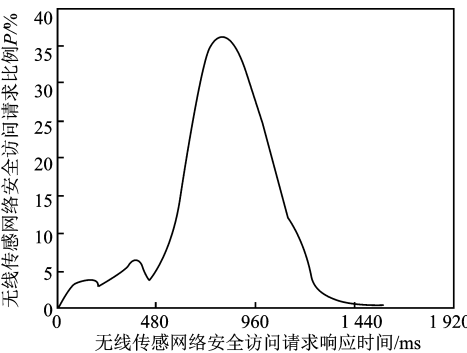


图2 文献[8]算法访问最大并发应用数量为 395 时的响应时间分布曲线

表2 访问响应时间超过 d 随多媒体应用并发个数的变化	
多媒体应用并发个数/个	访问响应时间超过 d /%
386	18
387	31
388	71
389	83
390	118
391	338

通过表 2 中的数据可以看出, 采用本文算法得

到的无线传感网络最大多媒体应用并发个数与实际应用结果十分接近, 显而易见, 本文提出算法的精确度和可靠性较高.

4 结束语

实验结果分析证明, 与其他算法相比, 本文算法在保证无线传感网络多媒体应用服务质量需求的基础上, 能够最大限度地利用无线传感网络存储系统中的服务资源, 同时通过调整改变约束性条件 d 和 p 能够适应服务质量不同等级的要求, 具有广泛的实用性价值.

参考文献:

[1] 刘雪艳, 张强, 李战明, 等. 面向智能电网通信系统的数据聚合和访问控制方法[J]. 电力系统自动化, 2016, 40(14): 135-144.

[2] 张悦, 郑东, 张应辉. 支持动态授权和文件评价的访问控制机制[J]. 计算机应用, 2015, 35(4): 964-967.

[3] 马萌, 唐卓, 李仁发, 等. 基于条件随机场的改进型 BLP 访问控制模型[J]. 计算机科学, 2015, 42(8): 138-144.

[4] 张欣晨, 杨庚. Hadoop 环境中基于属性和定长密文的访问控制方法[J]. 计算机工程与应用, 2015, 51(23): 87-93.

[5] 田野, 彭彦彬, 杨玉丽, 等. 无线体域网中基于属性加密的数据访问控制方案[J]. 计算机应用研究, 2015, 32(7): 2163-2167.

[6] 于会松, 孟照旭, 黄华晔, 等. 基于映射的角色访问控制模型的设计与实现[J]. 计算机仿真, 2016, 33(4): 292-295.

[7] 周明快. 基于 CP-ABE 的云计算改进属性加密安全访问控制策略设计[J]. 计算机测量与控制, 2015, 23(1): 297-299.

[8] 朱彦杰. 基于最优化网格分配的资源数据库访问控制[J]. 科技通报, 2015, 31(8): 216-218.

[9] 胡继荣. 气象雷达数据的传输方式和算法的基本研究[J]. 电子设计工程, 2016, 24(4): 125-127.

[10] 王文标, 葛占元, 汪思源, 等. 智能轨迹导引控制算法在电加热炉温度控制中的应用[J]. 科学技术与工程, 2015, 15(2): 250-253.

作者简介:

聂利颖 女, (1982-), 硕士研究生, 讲师. 研究方向为网络安全. E-mail: niliying788@163.com.

王婷婷 女, (1981-), 硕士研究生, 讲师. 研究方向为计算机网络.