流媒体系统多数据流安全的动态选择控制模型

肖 晨 马世龙 吕卫峰 王丽丰

(北京航空航天大学 计算机学院，北京 100191) (北京电子科技学院 电子信息工程系，北京 100070)

摘 要：部分加密等媒体数据加密算法是保护媒体数据安全的有效方法，但用其加密流媒体系统中的多路媒体数据将使系统面临效率、规模扩展与安全性问题.为此提出基于数据安全权重的多数据流加密的动态最优选择控制模型，根据各数据流的带宽、权重等参数，为不同数据动态选择不同强度的加密方法.由于化简后的数学模型是NP难的0-1背包问题，结合实际系统特点提出基于贪婪启发思想的增量式近似算法.理论分析和实验表明该算法时间复杂度低且具有良好的近似性.最终在一个实用流媒体系统——Admire系统中设计实现了选择控制模型的原型子系统.

关 键 词：流媒体系统；数据安全；部分加密；最优控制；近似算法

中图分类号：TP 309.2

文献标识码：A **文 章 编 号**：1001-5965(2008)11-1292-06

Selective control mechanism for multi-datastream security in streaming media system

Xiao Chen Ma Shilong Lü Weifeng

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Wang Lifeng

(Department of Electronic and Information Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Partial encryption and other media encryption schemes are effective approaches to encrypt the media data which are high volume and latency sensitive. However, use one media encryption scheme to protect all the media streams in a streaming media system will induce efficiency, scalability and security problems. To solve this problem, a security weightiness based dynamic optimal selective control mechanism for multi-datastream encryption was proposed. The idea of partial encryption was generalized from encrypting a subset of one stream to multi-streams. It can determine the optimum encryption algorithm with different security levels for each stream in the system, according to stream's bandwidth, weightiness and other parameters. Since the simplified mathematical model is 0-1 knapsack problem which is NP-hard, a greedy heuristic incremental approximate algorithm was designed. Theoretical and experimental analyses show the approximate rate and speed of the algorithm are effective enough to support real-time applications. A prototype was implemented in an actual video conferencing system: Admire.

Key words: multimedia system; security of data; partial encryption; optimal control; approximate algorithm

随着多媒体技术、网络通信技术的发展，视频会议、视频点播等流媒体系统被广泛研究[1-5].但网络安全问题给流媒体数据安全性构成了极大的威胁，成为上述系统中重要的问题与挑战[3-4].流

收稿日期：2007-09-26

基金项目：国家973资助项目(G1999032711,2005CB32190)；中央办公厅信息安全保密重点实验室基金资助项目(KYKF200702)

作者简介：肖 晨(1981—)，男，北京人，博士生，xiaochen@nlsde.buaa.edu.cn.

媒体数据带宽高、延迟敏感,其安全传输不同于文本等数据[6-7],从 20 世纪 90 年代中期开始针对音视频数据的加密优化方法[6-10]被广泛研究.其中一类方法利用音视频数据的编码特征和数据依赖关系,仅加密所有数据中的某一个重要子集,如 I 帧/块或 DCT 系数、运动向量等.即使攻击者获取其余未加密数据,也无法得到重要子集中的数据,从而难以重建原始音视频[7-9].另一类算法将变换编码与加密过程结合[10].由于上述方法需要使用特制的音视频编解码器,并存在安全隐患,且需要在安全与加密效率之间进行折中[4,11-12],因此难以在安全需求较高的保密应用中实用.

在多数据流的流媒体系统中固定使用一种加密方法,首先会限制系统规模的动态扩展,其次不能区分不同数据的重要程度,难以使重要数据获得较高安全性.因此美国 Argonne 国家实验室 AccessGrid 视频系统和国际电信联盟的 H.323 系统都建议对每个视频流采用不同强度的加密算法进行保护[5],但都未给出具体的选择控制方法.本文结合自主研发的 Admire[1-2] 流媒体系统定义了多数据流安全的最优选择控制问题,建立数学模型.因模型为 NP 难问题,进而研究近似求解算法,并在 Admire 系统中设计实现了原型子系统.

1　系统安全瓶颈及选择控制问题

1.1　流媒体系统结构及加解密处理瓶颈

流媒体系统中数据传输主要包括音视频、控制和应用数据[2,5].其中后者带宽相对媒体数据很小,因此本文集中讨论媒体数据的安全.

按照媒体数据分发方法可将系统结构分为组播和单播两类.组播结构包括 IP 组播和应用层组播[1],此类结构中媒体数据由底层组播路由器分发,分发网络一般不处理媒体数据.单播结构中数据由媒体网关负责分发[1-2],为扩展规模并充分利用客户端的有限带宽,网关常对媒体数据进行选择转发、转码、混音和混图等处理[2].

为保证数据通信的安全,媒体数据传输可用传统加密算法加密.但随着系统用户的增加,系统中某些节点上待加解密的数据带宽将大于加解密处理吞吐量,或造成加密延迟过大,使加密算法无法完成全部数据的实时加密[3,6].本文称之为媒体数据带宽与加解密吞吐量的不对称性,并称这些节点为加解密瓶颈.当系统用户规模较小时,不存在瓶颈节点,随着接入用户的增加,一些节点会首先成为瓶颈,本文称之为潜在瓶颈节点,这将影响系统接入用户数量,降低系统可扩展性.

在组播结构中,由于中间网络不处理媒体数据,因此潜在瓶颈节点是各会晤中接收数据最多的客户端.单播系统中由于媒体处理网关需要对媒体数据进行处理,收发数据都需要加解密,而客户端的数据量较小,因此潜在瓶颈节点是网关.

1.2　基于约束满足模型的选择控制问题

部分加密等音视频加密算法是一种解决不对称性的方法.但直接应用这些算法,如文献[3],会造成安全性与系统扩展性之间的折中.例如考虑一个简单的应用场景,共享组密钥的组播会晤中有 20 路数据媒体数据 $d_1 \sim d_{20}$,带宽都为 B,所有节点加解密吞吐量为 C,$2B<C<2.5B$.若对所有数据使用选择加密,如加密 10% 的数据,则系统中接收所有数据的客户端需要加解密的数据总量为 $B<C$,因此不存在加解密瓶颈.但该系统的问题在于:①系统规模无法扩展,例如当与会者增加到 25 人时,加解密带宽为 $2.5B>C$,会出现加解密瓶颈;②假设两路主发言节点数据 d_i 和 d_j 包含会议重要信息,由于保护不够,攻击者可通过对这两路数据的密码分析获得会议主要信息[11-12].

为了解决上述问题,本文定义如下的多数据流安全的最优选择控制问题:即在系统中不出现加解密瓶颈的约束下,最优化系统整体安全性.

例如对于前面例子,一种较优的方案是:对两路重要数据全部加密,余下数据使用加密比例较低的算法[7].由于加密资源始终被优先分配到两路重要数据,该方案能克服已有方案在安全性与扩展性上的缺陷:①当系统规模扩大到 25 人时,加解密数据总量仍约为 $2B<C$,不会产生加解密瓶颈;②由于重要数据被全加密,一般窃听无法取得任何信息,即使通过对其它数据的离线分析能还原出部分信息,但得不到会议的主要内容.

上述仅是一个极简单的场景.面对复杂的实际系统,选择控制会是一个更复杂的问题.为此,首先需要给出一套定量、可求解的动态最优选择控制模型,使计算机能自动求解.其次,由于流媒体系统的实时特性,需要设计快速求解算法.最后,需要在实际系统中设计实现最优选择控制子系统.后面 3 节将分别研究这 3 个问题.

2　最优动态选择控制的数学模型

本节提出解决前一节最优选择控制问题的数学求解模型.该模型利用系统中的控制节点统计各数据带宽,计算潜在瓶颈节点加解密各个流所消耗的加密资源,并根据各个数据的重要程度计

算其最优加密算法及加密强度，即模型中决策向量 $\boldsymbol{e}$ 和 $\boldsymbol{x}$. 决策变量将通过第 4.1 节中的控制信道发送到各个客户端，从而完成对数据加密的最优选择控制，使得多个数据流作为一个整体更加安全.

2.1 系统的通用最优选择控制模型

1) 数据及其带宽模型. 考虑一个由中心节点进行媒体数据处理转发的简化的单播流媒体系统. 在时刻 t 该系统由一个媒体转发处理网关、一个控制服务器以及 k_t 个客户端组成. 由于媒体网关需要处理所有媒体数据，因此它是数据加密的潜在瓶颈，本文集中讨论网关上的数据加解密.

时刻 t 系统 k_t 个客户端共产生 n_t 路媒体数据，用 n_t 维数据向量 $\boldsymbol{d}=(d_1,\cdots,d_{n_t})$ 表示，d_i 是逻辑上的第 i 路数据，它可能是由网关发送，或是由客户端发送并经服务器转发的一路数据的多份拷贝组成.

令向量 $\boldsymbol{b},\boldsymbol{c},\boldsymbol{r}$ 为 n_t 维向量，其中数据拷贝数向量 $\boldsymbol{c}=(c_1,\cdots,c_{n_t})$，$c_i$ 是数据 d_i 的拷贝个数；数据带宽向量 $\boldsymbol{b}=(b_1,\cdots,b_{n_t})$，$b_i$ 是数据 d_i 的带宽，并假定带宽恒定且可测量. 数据源向量 $\boldsymbol{r}=(r_1,\cdots,r_{n_t})$，若 d_i 的源是一个客户端，则 $r_i=1$，若是网关则 $r_i=0$. 全加解密数据 d_i，服务器需要解密的数据带宽为

$$b_{\mathrm{dec}}=b_i r_i \tag{1}$$

若服务器处理后分发的拷贝使用相同秘钥加密，则 c_i 个拷贝仅加密一次，服务器需加密的带宽为

$$b_{\mathrm{enc}}=b_i\cdot\min(c_i,1) \tag{2}$$

2) 加密吞吐量与延迟模型. 低延迟是实时流媒体系统的重要要求，为研究服务器上加解密吞吐量与延迟之间的关系本文做如下假设：①单位时间内请求加解密的报文个数服从 λ 的 Poisson 分布；②服务器上的软、硬件加解密的吞吐量 C 恒定且可测量，处理遵从先进先出；③报文长度 L_{p} 固定；④计算机存储器容量远大于 L_{p}，故近似认为队列长度 K 无穷. 上述假设与实际场景较接近且符合典型的 $M/M/1/K$ 排队系统[13]，由此可得平均排队延迟如式(3)，其中 λ 表示单位时间请求个数，$\mu=C/L_{\mathrm{p}}$，$\rho=\lambda/\mu$ 为负载率. 由式(3)可推出：给定平均排队延迟的上限 $l_{\mathrm{q}}^{*}>1/\mu$，则最大有效吞吐量 B 应满足式(4). 限于篇幅证明过程不赘述.

$$l_{\mathrm{q}}=[1+K\rho^{K+1}-(K+1)\rho^{K}]/[(1-\rho^{K+1})\cdot(\mu-\lambda)] \tag{3}$$

$$\left.\begin{aligned}&B<\alpha C\\&\alpha=1-[1/(\mu l_{\mathrm{q}}^{*})]\end{aligned}\right\} \tag{4}$$

3) 加密算法. 令集合 E 为音视频加密算法集合，E_k 为 E 中成员，表示 E 中某种加密算法. 当给定加密算法 E_k，则其安全加密率函数为 $g_{e_k}(x)$，值域为[0,1]，表示该算法在加密比率为 $x\in[0,1]$ 时提供的安全度，其中 1 最安全，$g'_{e_k}(x)\geqslant 0$. 常数 C_{enc,e_k} 和 C_{dec,e_k} 为加解密常数，表示算法 E_k 加密和解密单位数据消耗的加密处理能力(例如 DES，3DES 和 RC4 算法，该常数为 1，3 和小于 1 的正实数).

4) 决策变量与约束条件. 令向量 $\boldsymbol{e}$ 和 $\boldsymbol{x}$ 为 n_t 维向量，其中加密算法向量 $\boldsymbol{e}=(e_1,\cdots,e_{n_t})$，$e_i\in E$，是应用在第 i 路数据 d_i 上的加密算法. 加密比率向量 $\boldsymbol{x}=(x_1,\cdots,x_{n_t})$，其中 $x_i\in[0,1]$，是第 i 路数据 d_i 的加密比率. 由于选择控制模型是为不同的数据流选择不同强度的加密算法，因此向量 $\boldsymbol{x}$ 和 $\boldsymbol{e}$ 为最优化模型的决策变量. 根据式(1)、式(2)、式(4)以及上述变量，可得到约束表达式(5). 其含义为：网关上的所有加解密负载应当小于等于最大有效负载 αC.

$$\sum_{i=1}^{n_t}[(C_{\mathrm{enc},e_i}\min(c_i,1)+C_{\mathrm{dec},e_i}r_i)b_i x_i]\leqslant\alpha C \tag{5}$$

5) 安全权重向量. 令 $\boldsymbol{v}=(v_1,\cdots,v_{n_t})$ 为 n_t 维安全权重向量，其中 v_i 为已知正常数，表示第 i 路数据 d_i 的安全权重. 公平的衡量数据的安全权重是困难且带主观因素的工作，本文不深入展开，第 4 节原型系统中将给出较简单的权重计算方案.

6) 最优化目标函数：令 $F=f(y_1,\cdots,y_{n_t},v_1,\cdots,v_{n_t})$ 为系统多数据安全的目标函数，其中 $y_i=g_{e_i}(x_i)$ 表示第 i 路数据的安全级别. F 需满足 $\partial F/\partial y_i\geqslant 0$，故有：$\partial F/\partial x_i=(\partial F/\partial y_i)\cdot(\partial y/\partial x_i)=(\partial F/\partial y_i)\cdot(\partial g_{e_i}(x_i)/\partial x_i)\geqslant 0$，即数据加密比率增加，系统安全性不减. 由于 F 仅和加密算法向量 $\boldsymbol{e}$、数据加密比率向量 $\boldsymbol{x}$ 和安全权重向量 $\boldsymbol{v}$ 相关，该式可简单记为 $F=f(\boldsymbol{e},\boldsymbol{x},\boldsymbol{v})$.

7) 最优化表达式. 选择控制模型目的是在加密资源有限的情况下，为不同的数据流选择适当的加密算法，使得系统安全性最优，即在约束表达式(5)满足的情况下，使目标函数 F 最大化. 故最优表达式如式(6)，其中向量 $\boldsymbol{x}$ 和 $\boldsymbol{e}$ 为决策变量.

$$\left.\begin{aligned}&\max f(\boldsymbol{e},\boldsymbol{x},\boldsymbol{v})\\&\sum_{i=1}^{n_t}[(C_{\mathrm{enc},e_i}\min(c_i,1)+C_{\mathrm{dec},e_i}r_i)b_i x_i]\leqslant\alpha C\end{aligned}\right\} \tag{6}$$

2.2 简化后的模型

1) 加密算法集化简. 前面用 $g_{e_k}(x)$ 抽象定义

了加密算法的安全-加密率函数,然而定量给出它的解析形式是很困难的.例如对于部分加密算法 E_{PE}[6],其二阶导数 $g''_{e_{PE}}(x)$ 的取值与正负性等性质会极大地影响选择控制模型.为化简 $g_{e_k}(x)$,本文假设 $E=\{E_n,E_0\}$,其中 E_n 是一个全部加密算法(例如 DES),则 $g_{e_n}(x)\equiv 1, x=1$;E_0 表示不加密,则 $g_{e_0}(x)\equiv 0, x=0$;且有加解密常数皆为 1.因此 $g_{e_k}(x)\equiv x, x_i\in\{0,1\}$,从而可以消去函数 F 中的向量 $\boldsymbol{e}$,则 $F=f(x_1,\cdots,x_{n_t},v_1,\cdots,v_{n_t})$ 并简记为 $f(\boldsymbol{x},\boldsymbol{v})$.因此最优目标函数化简为 $\max f(\boldsymbol{x},\boldsymbol{v})$,其中 $\boldsymbol{x}$ 是唯一的决策变量,向量 $\boldsymbol{e}$ 可以通过判断 $\boldsymbol{x}$ 计算得到.

2) 具体化的安全函数.前面的最优化模型中没有给出目标函数的解析形式,为将该问题化简为线形规划问题,不妨取 $f(\boldsymbol{x},\boldsymbol{v})=\left(\sum x_i v_i\right)\Big/\sum v_i$,显然 $\partial F/\partial y_i = x_i\Big/\sum v_i \geqslant 0$,满足 F 的定义要求,且当所有 $x_i=1$ 则 $f(\boldsymbol{x},\boldsymbol{v})=1$,即当所有媒体数据被加密后系统最安全,反之最不安全,这是合理的.由于在任意给定时刻 t,$\sum v_i$ 为常数,因此 $\max\left(\sum x_i v_i\right)\Big/\sum v_i$ 等价于 $\max\sum x_i v_i$,即最优目标函数的最终化简形式.

3) 化简后的最优表达式.由于模型中向量 $\boldsymbol{b}$,$\boldsymbol{c}$,$\boldsymbol{r}$ 已知,若令 $\boldsymbol{w}$ 为 n_t 维向量,$w_i=(C_{enc,e_i}\cdot\min(c_i,1)+C_{dec,e_i}r_i)\cdot b_i$,并令 $M=\alpha C$,则式(6)化为

$$\left.\begin{aligned}&\max\sum_i(x_i v_i)\quad x_i\in\{0,1\}\\&\text{s.t.}\quad\sum_{i=1}^{n_t}(x_i w_i)\leqslant M\end{aligned}\right\}\tag{7}$$

上式为 0-1 背包问题的表达式[14],问题为 NP 难.

组播模型与单播系统类似,限于篇幅不赘述.

2.3　动态模型

前面模型是针对静态系统的,而实际系统中上述变量是动态变化的,本小节结合 Admire 流媒体系统研究动态系统中数据加密的选择控制.

由于前面已假设媒体数据流的带宽 b_i 可预测,因此 Admire 系统中仅以下 5 类事件会改变模型中相关参数:①系统内新增一路媒体数据 d_i.open;②减少一路媒体数据 d_i.close;③第 i 路数据增加一个接收者 d_i.addrecvr;④减少接收者 d_i.delrecvr;⑤强制或自动的权重变化 d_i.chngwt.其中事件①和②会使向量 $\boldsymbol{b},\boldsymbol{v},\boldsymbol{c},\boldsymbol{r}$ 的维数变化,事件③,④和⑤会直接或间接地影响第 i 路数据的安全权重 v_i.

当系统中发生上述任一事件,控制服务器通过安全的控制信道从客户端得到报告,并调整模型变量,此时最优化模型需要重新求解.

3　选择控制模型的近似求解算法

3.1　0-1 背包问题求解算法

1) 最优算法.第 2 节的研究将最优选择控制问题化简为 0-1 背包问题,该问题是一个 NP 难问题.其最优算法包括蛮力算法、回溯算法、分支定界算法以及动态规划算法等[14].蛮力算法的时间复杂度为 $O(2^n)$.回溯和分支定界算法是 2 种优化的算法,但在最坏情况下仍是指数时间复杂度.动态规划算法有 $O(nM)$ 的时间复杂度,但空间复杂度也高达 $O(nM)$,其中 M 是背包容积.

2) 近似算法.由于上述最优算法的计算复杂性高,而选择控制问题需要实时求解,因此需要考察近似算法.0-1 背包问题有多种基于贪婪启发策略的多项式时间近似算法,其核心思想分别是按照如下顺序选择物品:最大价值 $\boldsymbol{v}$,最小重量 $\boldsymbol{w}$ 或价值密度 v_i/w_i[15] 优先等.算法主要分为 2 个步骤:①对 $\boldsymbol{v}$,$\boldsymbol{w}$ 或 v_i/w_i 进行降序或升序排序(如快排序);②依次将重量 w_i 小于背包剩余负载的物品放入背包.因此近似算法的平均时间复杂度为 $O(n\log n)$[15].其中基于价值密度优先的算法[15]最常被使用,后面简称之为近似算法.

3) 近似算法近似度.记 $r_A(I_n)$ 为最大化问题的近似算法 A 在输入 I 且规模为 n 时的近似性态,$r_A(I_n)=v^*(I_n)/\text{val}(I_n,A(I_n))$,其中 $v^*(I_n)$ 为最优解,$\text{val}(I_n,A(I_n))$ 是近似解.当背包负载 $M>\max(w_i)$ 时,近似算法满足:$r_A<M/(M-\max(w_i))$,限于篇幅这里省略了证明过程,这说明如果 $\max(w_i)$ 远远小于 M,则在最差情况下近似解也将很接近最优解.在实际系统中 $w_i<1$ Mbit/s,$M>10$ Mbit/s,因此 $r_A(I_n)<1.12$,即在最差情况下近似解也能达到最优解的 90%.此外文献[15]指出实际中出现较差解的概率很低.

最优算法时间复杂度高,且由于模型中数据带宽等参数的测量存在误差,使最优算法决策准确的优势不明显,而近似算法近似度较好,因此研究选用近似算法作为 0-1 背包问题的求解算法.

3.2　增量式近似算法

第 2.3 节的动态模型指出系统中仅 5 种事件会引起模型状态及变量变化,且每个事件仅影响一路数据相关的变量,为此重新求解既浪费时间又没意义.本文设计了一种增量调整算法,使用折

半查找及插入代替排序，算法简述如下，改进后近似算法每次调整操作的时间复杂度为 $O(n)$.

增量式近似算法（输入：n, M, $\boldsymbol{v}$, $\boldsymbol{w}$, event；输出：$\boldsymbol{x}$）

switch event

case d_i.open：用折半查找将 d_i 按序插入数组

case d_i.close：删除对应项

case d_i.addrecvr ‖ d_i.delrecvr ‖ d_i.chngwt：使用折半查找调整 d_i 在排序数组中位置

for($j=1$；$j<n$；$j++$)//顺序访问，选择要加密的数据

if $w_j<M$ then select it：$x_j=1$；$M-=w_j$；

return $\boldsymbol{x}$； 算法结束

3.3 批量处理算法

当系统中状态变化极快时，服务器上频繁地选择控制以及控制通信会浪费控制服务器的计算与通信资源. 一种优化方法是采用事件批量处理，即定长时间间隔内的状态变化事件集中一次计算. 其优点是节省计算与通信资源，但会在一定程度上降低近似度. 本文将此作为一种备选方案.

4 原型系统与实验分析

4.1 原型系统的实现

在自主研发的 Admire 流媒体系统中实现了媒体数据加密的动态选择控制原型子系统，并应用于某安全项目. 图 1 给出了系统结构以及与选择控制相关的消息通信，控制服务器通过加密的私有控制信令与客户端通信完成选择控制.

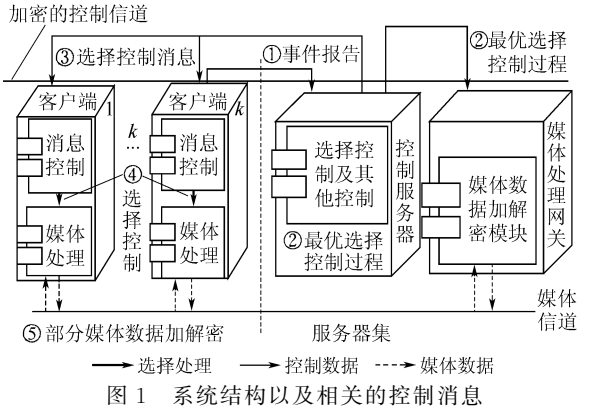

图 1 系统结构以及相关的控制消息

为减小对 Admire 系统其它模块的修改，将加解密过程实现在系统原有的通用网络复用模块 NSPD[2] 中. 该模块被用来作为 WinSPI 服务，替代原有的 WinSock 服务，并实现 NAT 防火墙的穿透功能[2]. 本文将加密的媒体数据报文作为 NSPD 载荷，并在 NSPD 报文头扩展位中用 1 位作为是否被加密的标志. 系统数据协议栈如图 2.

媒体数据		控制数据		应用数据
音频	视频	RTCP	AdmireMBus 控制信令	电子白板，录制回放，协同编辑，共享应用等
RTP 实时传输协议				
加密 NSPD 封装			数据加密	
UDP 协议			TCP 协议	
网络层，数据链路层，物理层				

图 2 增加数据加密及 NSPD 模块后的系统协议栈

由于应用的需要原型子系统其他设置如下，数据加密采用基于 PCI 总线的某型号加密卡实现，加密吞吐量 $C=12$ Mbit/s. 令 $l_q^*=5$ ms 则 $\alpha\approx 0.87$.

原型子系统中的权重设定为 $v_i=c_i v_{\text{conf}} v_{\text{chair}} \cdot v_{\text{a/v}}$. 其中 v_{conf} 是会议预设权重；音视频的 $v_{\text{a/v}}$ 设置分别是 2 和 1；由于 Admire 系统的会晤是基于主席控制模式的[1]，因此当数据由主席节点发出时 $v_{\text{chair}}=4$，否则为 1；c_i 是该路媒体数据被接收次数，这是考虑到关注者个数也反映了该数据的重要程度. 上述设置一般能使主席节点优先加密，接收者多的数据优先加密，音频优先于视频.

4.2 算法速度的测试结果

由于实际系统规模的限制，本文通过仿真程序研究各个背包求解算法的速度. 仿真程序用 C++语言编写，测试环境为 PIV 2.6 GHz，512 MB 内存的 WindowsNT 工作站. 由于近似算法的速度受 M, $\boldsymbol{w}$, $\boldsymbol{v}$ 取值影响很小，程序中的参数 w_i 及 v_i 分别取小于 1 000 和 200 的随机数，M 取值为 $\boldsymbol{w}$ 向量所有数据和的 40%，动态规划算法中取 $M=10\,000$. 表 1～表 3 中给出的试验结果为 100 次重复试验的平均时间.

表 1 蛮力算法与回溯算法的速度测试

问题规模	计算时间/s		问题规模	计算时间/s	
	蛮力算法	回溯算法		蛮力算法	回溯算法
8	<0.001	<0.001	20	0.265	0.040
12	0.001	<0.001	24	4.344	0.511
16	0.015	0.004	28	74.515	7.871

表 2 动态规划算法的速度测试

问题规模	计算时间/s	问题规模	计算时间/s
400	0.094	700	0.164
500	0.115	800	0.215
600	0.141	900	0.234

试验结果显示表 1 和表 2 的算法计算时间增长很快，难以满足实时系统要求. 增量算法在问题规模为 $n=2^{10}$ 时计算时间在毫秒量级，而增量式算法在问题规模为 $n\leqslant 2^{20}$ 时的计算时间约为近似

算法的 1/10,另外如图 3 所示,增量算法的计算时间增长较缓慢.由于 Admire 系统应用环境中节点一般小于 150,增量式算法完全能满足选择控制的实时要求.

表 3　近似算法与增量式近似算法的速度测试

问题规模	计算时间/s		问题规模	计算时间/s	
	近似算法	增量算法		近似算法	增量算法
2^{10}	<0.001	<0.001	2^{16}	0.078	0.008
2^{12}	0.004	<0.001	2^{18}	0.359	0.031
2^{14}	0.016	0.002	2^{20}	1.563	0.116

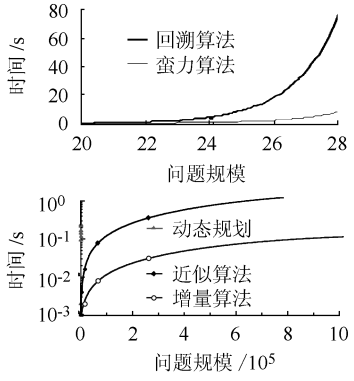

图 3　5 种算法计算时间增长趋势比较

5　结 束 语

高机密性流媒体系统中对多路媒体数据使用单一的视频加密方法进行保护将面临规模扩展和安全性问题.本文提出了多数据流安全的动态最优选择控制问题,并建立数学模型,根据各数据流的带宽、重要程度等参数它们动态选择不同强度的加密方法.其中基本模型普遍适用,简化模型更便于计算.由于简化模型是 NP 难的 0-1 背包问题,结合实际系统特点提出基于贪婪启发的增量式近似求解算法,理论分析和实验表明算法时间复杂度低且具有良好的近似性.最后在 Admire 系统中设计实现了选择控制模型的原型子系统.

参考文献 (References)

[1] Jin T, Sheng X Z, Lu J. Admire, a prototype of large scale e-collaboration platform[C]//Li M L. Grid and Cooperative Computing, Lecture Notes in Computer Science (LNCS) 3033. Berlin:Springer-Verlag,2003:335－343

[2] Huang T, Yu X N. An adaptive mixing audio gateway in heterogeneous networks for admire system [C]//Li M L. Grid and Cooperative Computing, Lecture Notes in Computer Science (LNCS) 3033. Berlin:Springer-Verlag,2003:294－302

[3] Yin H, Lin C, Qiu F,et al. CASM: A content-aware protocol for secure video multicast[J]. IEEE Trans on Multimedia,2006,8(2):270－277

[4] Liu F W, Koenig H. A novel encryption algorithm for high sesolution video [C]//Proc of NOSSDAV05. New York: ACM Press,2005:69－74

[5] ITU-T H. 235(v3). Security and encryption for h-Series (H. 323 and other H. 245-based) multimedia terminals[S]

[6] Maples T, Spanos G. Performance study of a selective encryption scheme for the security of networked, real-time video[C]//4th Int Conf on Computer Comm and Networks. Wash. D C: IEEE Computer Society Press,1995:2－10

[7] Tang L. Methods for encrypting and decrypting MPEG video data efficiently[C]//Proceedings of the 4th ACM International Conference on Multimedia. Boston, MA: ACM Press, 1996:219－230

[8] Servetti A, Martin J C. Perception-based partial encryption of compressed speech [J]. IEEE Trans on Speech and Audio Processing,2002,10:637－643

[9] Cheng H, Li X B. Partial encryption of compressed images and videos[J]. IEEE Trans on Signal Processing,2000,3: 2439 2451

[10] Tosun A S, Feng W C. On error preserving encryption algorithms for wireless video transmission[C]//Proc of the 9th ACM International Conference on Multimedia. New York:ACM Press,2001: 302－308

[11] Lookabaugh T, Sicker D C, Keaton D M, et al. Security analysis of selectively encrypted MPEG-2 streams [C]//Proc of the Multimedia Systems and Applications VI. Bellingham: SPIE Press, 2003:10－21

[12] Qiao T L, Narhstedt K. Comparison of MPEG encryption algorithms[J]. Computer and Graphics,1998,22 (4): 437－448

[13] Robertazzi T G. Computer networks and system: queuing theory and performance evaluation[M]. Berlin: Springer, 2000

[14] Martello S, Toth P. Knapsack problems: algorithms and computer implementations[M]. Chichester: John Wiley & Sons, 1990

[15] Sahni S. Approximate algorithms for the 0-1 knapsack problem [J]. Journal of the Assoc for Computing Machinery, 1975,22(1):115－124

(责任编辑:文丽芳)