基于P2P网络的机顶盒VoD系统条件接收机制

周 璇[1] 宦国强[2] 宋占杰[1,2]
(天津大学电视与图像信息研究所 天津 300072)[1] (天津大学理学院 天津 300072)[2]

摘 要 近年来,基于对等网络(Peer-to-Peer,P2P)的视频点播(Video-on-Demand,VoD)作为付费网络电视业务的一种新趋势受到了越来越多的关注,然而对等网络自身存在的不稳定性、异构性等缺陷,导致这种系统存在较大的信息安全隐患,从而严重阻碍了其推广使用。基于P2P网络的机顶盒VoD系统条件接收机制分析了现有系统的不安全因素及问题症结,提出了一种适用于P2P网络的VoD系统动态双向条件接收(Conditional Access,CA)机制,通过采用双向认证协议来保证通信双方身份的可靠性。同时在身份认证中可以结合密钥协商,生成用于传输控制字的业务密钥。另外,在简化设计的同时,也进一步提高了系统的安全性。

关键词 对等网络,视频点播,条件接收,双向认证,密钥协商
中图法分类号 TP393.04 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.013

Conditional Access Mechanism of Video-on-demand System Based on Peer-to-Peer Network

ZHOU Xuan[1] HUAN Guo-qiang[2] SONG Zhan-jie[1,2]
(Television and Image Information Institute, Tianjin University, Tianjin 300072, China)[1]
(School of Science, Tianjin University, Tianjin 300072, China)[2]

Abstract Video-on-demand (VoD) based on Peer-to-Peer (P2P), as a new trend of the pay-IPTV service, has caused widespread concern in recent years. However, the instability and heterogeneity of the P2P network causing the existence of information security risks impede the realization of this system. On basis of conditional access mechanism of Video-on-demand system based on Peer-to-Peer network, we analyzed the insecurity factors of traditional system and proposed a kind of dynamic and two-way conditional access mechanism which is suitable for VoD system based on P2P. Mutual authentication protocol ensures the reliability of the identity of the communicating parties and generates the service key for transmitting control word, combing with the key agreement. This mechanism simplifies the design of system, and further improves the security of the system.

Keywords Peer-to-Peer, Video-on-demand, Conditional access, Mutual authentication, Key agreement

1 引言

IPTV作为一种新型的网络服务,近年来得到迅猛发展。IPTV通过IP网络传播电视节目、音视频资源和一些交互式节目等。典型的IPTV服务包括在线电视、视频点播(VoD)、时移电视等[1]。在所有IPTV提供的服务中VoD服务是对IPTV供应商最重要的服务之一,受到了广泛关注。因此,提供一个高安全、高收益、高质量的VoD系统非常重要。

VoD系统改变了传统电视人机交互性差的缺陷,开启了互联网电视的新时代。最初的VoD系统基于C/S结构,侧重解决增加系统支持的用户量并降低用户的等待时间等一系列问题[2];随后出现了基于对等网络(P2P)的VoD点播系统,这一系统的出现使得VoD系统实现了真正意义上的即时播放,并成为基于IP的VoD系统网络架构的主流[3,4]。VoD产业在取得很大成就的同时,也面临着许多困难,VoD产业的发展出现了"驻点现象",即用户量无法快速增长。造成这一结果的很大一部分因素就是网络环境难以保障节目内容的安全性[4]。现有的VoD系统中,为了保护节目的版权,广泛采用的方法是:在客户端采用数字版权管理(Data Right Management,DRM)技术,DRM保护技术使用以后可以控制和限制数字化媒体内容的使用权的方法,从技术上防止数字媒体的非法复制,或者在一定程度上使复制很困难,最终用户必须得到授权后才能使用数字媒体[5]。但是实践证明这种DRM保护技术仍然存在诸多缺陷。本文在传统的DRM技术的基础上,结合条件接收(Conditional Access,CA)机制来更有效地保护点播节目的版权。

针对IPTV中的CA系统目前已经提出很多不同的方案,如基于IC卡的CA系统和软件CA系统。基于IC卡的CA系统较为成熟,该系统将加密解密、加扰、解扰等模块放入一张可插拔的有独立操作系统的IC卡上,使具体的解密、

到稿日期:2014-05-19 返修日期:2014-09-23 本文受国家自然科学基金(61379014)资助。
周 璇(1989—),女,硕士生,主要研究方向为计算机网络通信、流媒体传输、数字电视条件接收系统,E-mail:zhouxuan@tju.edu.cn;宦国强(1992—),男,硕士生,主要研究方向为计算机网络、模式识别;宋占杰(1965—),男,博士,教授,主要研究方向为随机信号压缩采样及统计分析、随机过程采样、重构与逼近等。

解码与 IPTV 终端分离[6]。虽然这种方式自诞生以来得到广泛使用，但其缺陷也是显而易见的，即现有的终端必须与某家特定的 CA 系统绑定生产和销售。软件 CA 系统把加密体系建立在通用运算平台上，依靠软件可以不断更新的特点，通过网络可对加密算法、密钥进行实时更换。软件加密体系避免了硬件加密体系被动的局面，安全性更高，成本更低[6]。这种方式目前主要集中在节目密钥管理机制的研究，如基于 Logistic 混沌映射技术[6]、DCAS 技术[7]等。由于 P2P 网络架构的特殊性，完全将上述方案移植到 VoD 系统中必然存在风险。本文提出一种适用于 P2P 网络环境的 VoD 系统条件接收机制，充分考虑点播节目的各个环节：用户的鉴权/授权、节目的加密/解密以及密钥的管理，从而实现节目资源仅被各个授权节点安全共享。

2 系统方案

CA 系统在付费电视市场举足轻重，所谓 CA 系统保证业务仅被授权接收的用户所接收，其主要功能是对信号加扰、对用户电子密钥的加密以及建立一个确保被授权的用户能接收到加扰节目的用户管理系统[6]。然而 CA 系统自诞生以来并没有对其结构和发展做出非常明确的定义，主流的 CA 系统结构均采用在 ITU-810 中提出的 3 层密钥层次结构：MPK、AK 和 CW[1,8]。这 3 层密钥是设计一个安全的条件接收系统的关键，如图 1 所示。PRG 是指扰码序列生成器，在头端，其初始条件受制于控制字 CW，扰码序列是伪随机二进制序列，用于对发送的视频节目进行加扰，根据这个原理，只要接收端有一个相同的扰码生成器，同时将 CW 发送给接收端用于控制该扰码器，运用对应的解扰算法就可以对相应的信息流解扰恢复出原始信号。后两层加密的过程就是为了实现将 CW 安全传送并达到授权控制的目的。使用授权密钥 AK 对 CW 加密形成授权控制信息 ECM，同时，使用分配密钥 MPK 对 AK 加密形成授权管理信息 EMM。ECM、EMM 和加扰的节目被复用到 TS 传送流当中。用户管理系统负责更新 MPK 和用户信息。

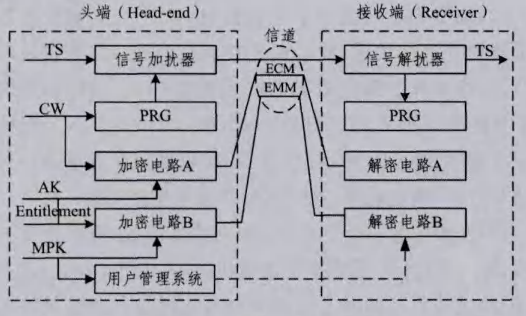

图 1 条件接收系统框图

基于上述框架，本文提出的 CA 机制主要包含以下 3 个部分：

(1)头端 VoD 资源服务器：提供 VoD 服务的业务，主要包括电视节目、音视频资源等；

(2)接收端对等用户：对等用户为允许接收 IPTV 业务的机顶盒，为了实现安全共享，这种机顶盒改变了传统的 IC 卡和机顶盒通信模式，采用嵌入式 CA 技术，将原始的智能卡换成机顶盒内置的有唯一 ID 的高级安全加密芯片；

(3)接收端调度节点：该节点和 VoD 服务器动态建立连接，负责调度业务的分发。

本文提出的 CA 机制主要包含以下几个环节：(1)用户注册登录；(2)节目分块加扰；(3)授权密钥生成；(4)节目分发；(5)节目解密观看。

2.1 用户注册登录

对用户而言，现有的 VoD 系统大部分都被集成在机顶盒中成为一种受 DRM 技术保护的应用软件[4]，因此我们后续的工作都是在此基础上展开。用户授权包含两个阶段，一方面，用户在收看付费节目之前，需要在远程的用户管理系统中进行注册；另一方面，用户点播节目之前要完成登录授权和双向认证，只有通过了登录认证之后，才可授权点播业务，如图 2 所示。

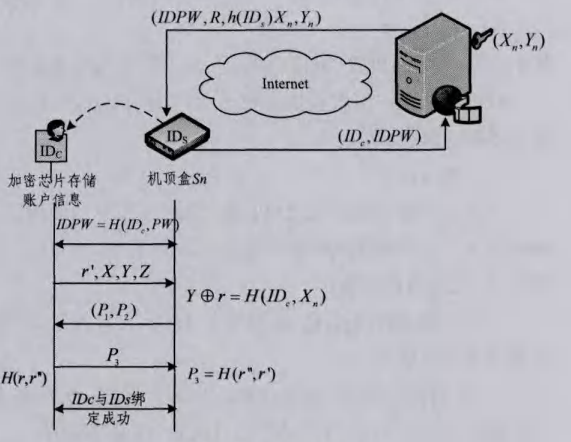

图 2 用户注册登录

用户注册阶段：当一个新的用户申请观看付费节目时，需要提供其身份 ID，这里涉及双重 ID，一重是机顶盒生产时的唯一标识 ID_s；另一重是机顶盒加密芯片中存储的用户个人的账户信息 ID_c，在加密芯片中还存储有账户密码 PW。加密芯片结合一定的驱动程序实现账户鉴权。用户端机顶盒计算 $IDPW=H(ID_c, PW)$，其中，$H(\cdot)$是一种单向抗碰撞 Hash 函数，只有加密芯片和机顶盒知道。将 ID_c 和 $IDPW$ 发送至前端用户管理系统，用户管理系统计算 R 值，$R=ID\text{-}PW \oplus H(ID_c, X_n)$，$Y_n=g^{X_n} \bmod p$，其中 X_n 是机顶盒的私钥，由前端的用户管理系统决定，Y_n 是生成公钥，p 为任意质数。将 $IDPW$、R、$H(ID_s)$和(X_n, Y_n)等一些账户信息存储在机顶盒加密芯片中，并通知用户，其中 $h(\cdot)$是一种单向抗碰撞 Hash 函数，输出长度一般设定为 128bit；

用户登录阶段：用户登录阶段需要完成本地认证、双向认证和密钥协商 3 个步骤。

(1)本地认证：检查 $IDPW=H(ID_c, PW)$，如果等式不成立，则拒绝登录请求；否则，本地登录允许，此时机顶盒会生成一个随机序列 r，长度为 512bit，按照如下规则计算 r'，X，Y，Z，K，并发送给机顶盒。

$$r'=H(h(ID_c), r) \tag{1}$$

$$X=R \oplus IDPW \tag{2}$$

$$Y=X \oplus r \tag{3}$$

$$Z=r \oplus h(ID_S) \tag{4}$$

$$K=ID_c \oplus r' \tag{5}$$

(2)双向认证：当接收到登录请求时，机顶盒和加密芯片

之间应按照以下步骤实现双向认证，这一步的目的是实现机顶盒和账户的绑定。

1)机顶盒得到(Y,Z,K)后按照如下规则计算r和r'：

$$r=Z\oplus h(ID_s) \tag{6}$$

$$r'=H(h(ID_s),r) \tag{7}$$

2)机顶盒计算$ID_c=K\oplus r'$获得账户信息；

3)机顶盒计算$X=Y\oplus r$，并检查下述等式是否成立：

$$\begin{aligned}Y\oplus r&=R\oplus IDPW\\&=IDPW\oplus H(ID_c,X_n)\oplus IDPW\\&=H(ID_c,X_n)\end{aligned} \tag{8}$$

4)如果上述等式不成立，则机顶盒拒绝和当前账户通信；否则机顶盒接受账户登录请求并计算：

$$P_1=H(r',h(ID_s))\oplus r'' \tag{9}$$

$$P_2=H(r,r'') \tag{10}$$

其中，r''为一个随机数，机顶盒将(P_1,P_2)发送给加密芯片；

5)机顶盒账户鉴权模块计算$r''=P_1\oplus H(r',h(ID_s))$检查下述等式是否成立：

$$P_2=H(r,r'') \tag{11}$$

6)如果上述等式不成立，机顶盒拒绝该账户的使用，账户和机顶盒绑定失败；否则账户鉴权模块计算$P_3=H(r'',r')$，并将P_3发送给机顶盒；

7)最后机顶盒检查P_3是否等于$H(r'',r')$，若是，则账户和机顶盒绑定成功。

(3)密钥协商：如果机顶盒和账户绑定成功，双方生成一个会话密钥$SK=H(r',r'',ID_c,h(ID_s))$，并通知双方。

2.2 节目分块加扰

如图3所示，在VoD视频分发中一个完整的视频资源被分成若干块，每一块被不同的控制字加扰。通过对每一块资源的控制字进行加密，形成授权控制信息，这样就可以将加扰的节目块和授权控制信息通过P2P网络进行传输。

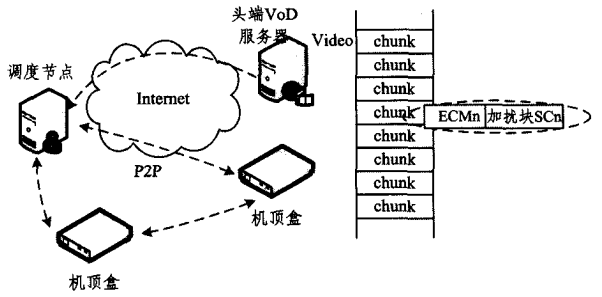

图3 节目分块加扰与传输

每一个加扰块SC_n的控制字CW_n是随机生成的。头端服务器使用其公钥Y_{VoD}和加密种子数z来加密控制字CW_n，加密过程如下：

$$ECM_n=CW_n\cdot Y_{VoD}^z \bmod p, n\in[1,N] \tag{12}$$

其中，p为任意质数。为了提高安全性，VoD服务中每个节目的加密种子数z应该不同。同时，为了在各个节点共享节目时鉴定资源的合法性，计算加扰块SC_n和授权控制信息ECM_n的Hash值：

$$\gamma_n=h(SC_n\parallel ECM_n), n\in[1,N] \tag{13}$$

2.3 授权密钥生成

(1)假设用户账户认证通过，各个节点用户可以请求节目，对于VoD服务，节点用户请求服务需要提供节目序列号SN；

(2)根据节点用户S_n的请求，利用通信种子数z生成如下两个数值：

$$a_n=(Y_n^z)/(Y_{VoD}^z) \bmod p \tag{14}$$

$$b=g^z \bmod p \tag{15}$$

其中，a_n和b构成授权管理信息$EMM=(a_n,b)$，并发送至节点S_n；

(3)机顶盒从服务供应商收到授权管理信息，使用私钥X_n生成授权密钥AK：

$$\begin{aligned}AK&=a_n/b^{X_n} \bmod p\\&=(g^{X_n\cdot z})/(Y_{VoD}^z\cdot g^{X_n\cdot z}) \bmod p\\&=Y_{VoD}^{-z} \bmod p\end{aligned} \tag{16}$$

2.4 节目分发

为了实现P2P网络下视频节目的有序实时播放，在接收端需要使用一个调度节点来管理视频节目的共享和交换。整个过程如图4所示。

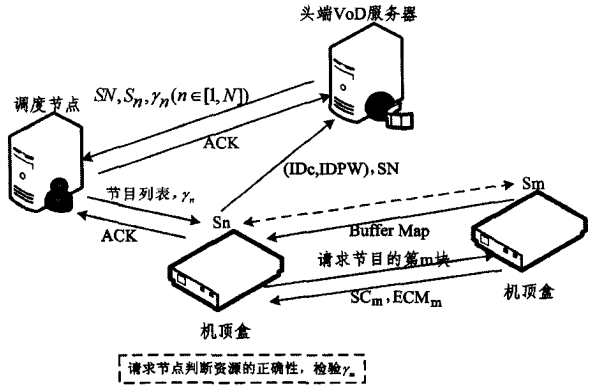

图4 VoD点播

(1)某节点用户请求VoD资源，该节点机顶盒记为S_n，服务器响应该节点机顶盒的请求，将节目资源序列号SN以及该资源的Hash值$\gamma_n(n\in[1,N])$传输并保存在调度节点中；

(2)调度节点响应一个应答信息ACK给头端服务器表示确认建立连接关系，此后调度节点会处理一系列接收端用户节点，这些节点都包含VoD节目数据段的一部分，同时包含节目的节点列表和节目的Hash值$\gamma_n(n\in[1,N])$也传输并保存在机顶盒S_n中；机顶盒S_n接收到包含点播节目数据段的节点表，随机选择一些节点，并建立连接关系；

(3)如果任意一个节点S_m和当前节点S_n成功建立连接关系，S_m会将自己的缓冲区数据映射表(buffer map)发送给S_n，缓冲区映射表标识了当前节点可从此建立连接关系的节点得到哪些数据块，通过此映射表S_n可以确定点播VoD加扰块的分布，并向目标节点请求该加扰块；

(4)假设S_n请求S_m提供第m段节目，此时需要将授权控制信息ECM_m和加扰块SC_m拷贝到节点S_n中；

(5)为了确保接收(SC_m,ECM_m)的准确性和完整性，可以利用S_n从超级节点处得到的Hash值γ_m来判断$\gamma_m=h(SC_m\parallel ECM_m)$等式是否成立。

2.5 节目解密播放

如1.2节所述，VoD资源的每个节目被分成若干块，每

块利用控制字 CW_n 加扰，同时利用授权控制信息 ECM_n 来保护控制字 CW_n。在节目解密播放过程中，每一个加扰块 SC_n 利用 CW_n 解扰，需要使用授权密钥 AK 解密控制字 CW_n，过程如下：

$$ECM_n \cdot AK \bmod p = CW_n \cdot Y_{VoD}^{\tilde{x}} \cdot Y_{VoD}^{-\tilde{x}} \bmod p = CW_n \tag{17}$$

解密控制字之后，使用密钥协商生成的账户和机顶盒之间的会话密钥对控制字加密，形成 $CW_n' = E_{SK}(CW_n)$，将 CW_n' 发送给机顶盒。对于每一个加扰块 SC_n，在播放过程中利用其对应的控制字 $CW_n = D_{SK}(CW_n')$ 解扰，实现节目的正常播放。

3 系统性能分析与测试

本文提出的基于 P2P 网络下的 VoD 系统条件接收机制有效地保护了 VoD 服务供应商的权益以及 VoD 资源的版权，特别是在涉及付费 VoD 业务领域，这种机制的优势更为明显。下面从安全性和可行性两方面对本文提出的条件接收机制进行分析。

3.1 系统安全性分析

(1)增加了用户注册和登录，用户账户和机顶盒的绑定，这样可以保证通信双方身份的可靠性。在用户注册过程中将账户信息 ID_c 和 $IDPW$ 发送到用户管理系统，发送 $IDPW = H(ID_c, PW)$，没有直接发送 PW。$H(\cdot)$ 使用具有单向抗碰撞的 Hash 函数，使得 ID_c 和 $IDPW$ 的破解十分困难；另一方面，构造 $H(ID_c, PW) = IDPW$ 也几乎是不可能的。

(2)采用 ITU-810 中提出的 3 层密钥层次结构(CW, AK, MPK)，这 3 层密钥结构的核心是保护控制字 CW。本文提出的这种条件接收机制将 VoD 资源分块加扰，对于每块资源使用不同的控制字加扰，解密控制字的过程中，只有正确的私钥 X_n 才能从授权管理信息 EMM_n 中获得正确的授权密钥 AK。

(3)在控制字 CW 的传输过程中，使用协商的会话密钥 SK 对其加密和解密。会话密钥 $SK = H(r', r'', ID_c, h(ID_s))$ 可以保证几乎每次会话生成的会话密钥 SK 都是不同的，这样控制字的破解概率极低。

3.2 系统可行性分析

从整个节目点播的流程可以看出，用户观看 VoD 服务提供的视频首先需要获得授权密钥 $AK = Y_{VoD}^{-\tilde{x}} \bmod p$，该过程在点播节目开始，只需要执行一次指数运算。获得授权密钥之后，需要使用该授权密钥解密授权控制信息 ECM_n 以得到每个加扰块的控制字 $CW_n = ECM_n \cdot AK \bmod p$，这一过程只需执行一次乘法运算。因此，本文提出的条件接收机制在现有的机顶盒和计算机的硬件条件下是可行的。

3.3 不同系统效果比对与测试

一个基于 P2P 网络的安全的资源版权保护系统需要授权、鉴权、内容加密和解密以及密钥管理[9,10]。文献[11]提出的方法只考虑了内容的加密以及鉴权；文献[12]提出的方法侧重于密钥管理，将用户分为 3 类，针对每一类用户使用不同的密钥更新机制。对比这些机制，本文提出的这种版权保护系统使用了基于 3 层密钥结构的条件接收机制，私钥 X_n 只有授权用户才可以使用；传输的内容采用了两步加密/解密；动态密钥协商保证通信双方身份的可靠性。对比结果如表 1 所列。

表 1 对比不同的 P2P-VoD-DRM 方法

方法	授权	鉴权	内容加密/解密	密钥管理
文献[11]的方法	无	有	有	无
文献[12]的方法	无	无	无	有
本文的方法	有	有	有	有

根据本文提出的方案，搭建基于 P2P 的 VoD 点播系统进行测试，节点使用基于海思 Hi3716C 平台的高清互动机顶盒，头端使用 Dell PowerEdge R410 Server -Intel Xeon E5630 2.53GHz 的机架式服务器。用户信息的 Hash 函数使用 BKDRHash 测试冲突率。测试数据 1 使用 100000 组数据，其中包含字母和数字；测试数据 2 使用 100000 组数据，其中仅包含字母，实验结果如表 2 所列。

表 2 用户信息 Hash 冲突次数

测试项	数据 1	数据 2
BKDRHash	2/100000	0/100000

节目加密测试使用 200M 的视频文件，以 4KB 的块为大小计算 MD5 值，并以此作为 Hash 关键字，Hash 函数同样使用 BKDRHash，测试散列分布性和平均桶长。使用 10240 的桶，调用 50000 次，实验结果如表 3 所列。

表 3 节目加密的散列分布性和平均桶长

测试项	散列分布率	平均桶长
BKDRHash	98.87%	4.5

从表 2 和表 3 的数据可以看出，本文提出的机制的冲突率较小，从而可以确保一定范围内的用户授权信息和节目内容具有较高的安全性。

结束语 本文提出一种基于 P2P 网络的 VoD 系统条件接收机制。这种机制对于 P2P 网络具有良好的适应性。P2P 网络一方面可以保证在各个用户之间自动地完成视频内容的传播，从而避免了所有用户从一个或几个服务器获取资源而引起网络拥塞，这样可以大大减少服务提供商的负荷；另一方面，本文提出的这种条件接收机制充分考虑了视频传输和播放的保密性、完整性以及系统的可行性，不仅考虑了密钥管理，而且使基于 P2P 网络的 VoD 服务的安全性和有效性得以保证。在今后的研究工作中，一方面可以考虑将该方案进行扩展，使其适用于整个 IPTV 业务，同时可以考虑将该方案平移到有线数字电视业务中，发展无卡条件接收技术；另一方面随着节点用户的增多，可以考虑通过多重 Hash 运算来获得更高的安全性。

参 考 文 献

[1] Lee J, Rhee H, Lee D. Efficient and Secure Communication between Set-top Box and Smart Card in IPTV Broadcasting[C]// IEEE International Conference on Convergence and Hybrid Information Technology. 2008: 307-310

[2] 沈时军，李三立. 基于 P2P 的视频点播系统综述 [J]. 计算机学报，2010，33(4)：613-624

(下转第 100 页)

WSN 的性能有一定的应用背景和实际意义。EH-WSN 的路由算法对于网络运行的持续性和网络性能的提升有很大的影响，结合 EH-WSN 节点能量捕获的特性，在路由发现时考虑链路的成功收包率，为节点配置合适的传输速率，有利于确保传输质量、减少传输时延和提高网络的吞吐率。从实验的结果来看，所提出的方法是可行的和有效的。

参 考 文 献

[1] Shuai Peng, Chor Ping Low. Energy Neutral Routing for Energy Harvesting Wireless Sensor Networks[C]// Proceedings of 2013 IEEE Wireless Communications and Networking Conference (WCNC). Shanghai, 2013: 2063-2067

[2] Kawashima K, Sato F. A Routing Protocol Based on the Power Generation Pattern of Sensor Nodes in Energy Harvesting Wireless Sensor Networks[C]// Proceedings of 2013 16th International Conference on Network-Based Information Systems (NBiS). Gwangju, 2013: 470-475

[3] Nga Dang, Roshanaei M, Bozorgzadeh, et al. Adapting Data Quality with Multihop Routing for Energy Harvesting Wireless Sensor Networks[C]// Proceedings of 2013 International Green Computing Conference (IGCC). Arlington, 2013: 1-6

[4] Xiao Meng, Zhang Xue-dan, Dong Yu-han. An Effective Routing Protocol for Energy Harvesting Wireless Sensor Networks[C]// Proceedings of 2013 IEEE Wireless Communications and Networking Conference (WCNC). Shanghai, 2013: 2080-2084

[5] Beheshtiha S S, Tan H, Sabaei M. Opportunistic Routing with Adaptive Harvesting-aware Duty Cycling in Energy Harvesting WSN[C]// Proceedings of 2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC). Taipei, 2012: 90-94

[6] Alrajeh N A, Han S U, Lloret J, et al. Secure Routing Protocol Using Cross-Layer Design and Energy Harvesting in Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2013, 2013: 1-11

[7] Eu Z A, Tan H-P. Adaptive Opportunistic Routing Protocol for Energy Harvesting Wireless Sensor Networks[C]// Proceedings of 2012 IEEE International Conference on Communications (ICC). Ottawa, 2012: 318-322

[8] LAN/MAN Standards Committee. Part 15. 4: Low-Rate Wireless Personal Area Networks[S]. 2012

[9] Ali M I, Al-Hashimi B M, Recas J, et al. Evaluation and Design Exploration of Solar Harvested-Energy Prediction Algorithm [C]// Proceedings of 2010 Design, Automation & Test in Europe Conference & Exhibition (DATE). Dresden, 2010: 142-147

[10] Chin Keong-Ho, Pham Dang Khoa, Pang Chin Ming. Markovian Models for Harvested Energy in Wireless Communications[C]// Proceedings of 2010 IEEE International Conference on Communication Systems (ICCS). Singapor, 2010: 311-315

[11] Ventura J, Chowdhury K. Markov Modeling of Energy Harvesting Body Sensor Networks[C]// Proceedings of 2011 IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC). Toronto, 2011: 2168-2172

[12] Heinzelman W B, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Trans on wireless communications, 2002, 1(4): 660-670

[13] Landolsi M A, Stark W E. On the accuracy of Gaussian approximations in the error analysis of DS-CDMA with OQPSK modulation[J]. IEEE Transactions on Communications, 2002, 50 (12): 2064-2071

[14] Perkins C, Belding-Royer E, Das S. Ad hoc On-Demand Distance Vector (AODV) Routing[OL]. http://moment. cs. ucsb. edu/AODV/

[15] Vuran Mehmet C, Akyildiz I F. Cross-Layer Analysis of Error Control in Wireless Sensor Networks[C]// Proceedings of 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks. Reston, 2006: 585-594

[16] Seah W K G, Zhi Ang Eu, Tan H. Wireless Sensor Networks Powered by Ambient Energy Harvesting (WSN-HEAP)-Survey and Challenges[C]// Proceedings of 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. Aalborg, 2009: 1-5

[17] Wu Yin, Liu Wen-bo. Routing protocol based on genetic algorithm for energy harvesting-wireless sensor networks[J]. IET Wireless Sensor Systems, 2013, 3(2): 112-118

（上接第 75 页）

[3] Hei Xiao-jun, Liu Yong, Ross K W. IPTV over P2P streaming networks: the mesh-pull approach [J]. Communications Magazine, 2008, 46(2): 86-92

[4] Chen Y-F, Huang Yen-nun, Jana R, et al. Towards capacity and profit optimization of video-on-demand services in a peer-assisted IPTV platform [J]. Multimedia Systems, 2009, 15(1): 19-32

[5] Xu C, Li S. Digital rights management solutions based on IPTV DRM[C]// 2010 2nd International Conference on Networking and Digital Society (ICNDS). IEEE, 2010, 2: 43-46

[6] 陈粒，王汝传，李致远，等. 基于 P2P 的 IPTV 的 CAS 密钥管理机制[J]. 计算机与数字工程，2010，38(11)：100-103

[7] Moon J, Kim J, Park J, et al. A dynamic conditional access system for IPTV multimedia systems[C]// Fourth International Conference on Systems and Networks Communications, 2009 (ICSNC'09). IEEE, 2009: 224-229

[8] Wang Chun-ling, Feng Jing-yu. A Study of Mutual Authentication for P2P Trust Management[C]// 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). IEEE, 2010: 474-477

[9] 王真，张志勇，常亚楠. 一种面向 Android 平台的多媒体数字版权管理系统[J]. 计算机科学，2014，41(5)：129-132，142

[10] Wu Wei-chen, Chen Yi-ming. A anonymous DRM scheme for sharing multimedia files in P2P networks[J]. Multimedia Tools and Applications, 2014, 69(3): 1041-1065

[11] Liu Xiao-yun, Huang Tie-jun, Huo Long-she, et al. A DRM architecture for manageable P2P based IPTV system[C]// 2007 IEEE International Conference on Multimedia and Expo. IEEE, 2007: 899-902

[12] Zhang Yuan, Huang Yong-feng, Yuan Jian. An efficient group rekey scheme for P2P IPTV DRM system[C]// 2011 13th International Conference on Advanced Communication Technology (ICACT). IEEE, 2011: 1479-1483