基于SRP算法的安全AODVjr协议

梁滋璐，夏侯士戟，陈东义

(电子科技大学移动计算研究中心 成都 610054)

【摘要】无限传感器网络由大量具有微处理能力的传感器节点组成，对物理环境参数进行各种监控。路由是无限传感网络中的一个重要问题，路由协议用于实现各种路由功能。AODVjr协议是应用最为广泛的无限传感器网络路由协议。作为AODV协议的简化，AODVjr协议省略了AODV协议中的各项优化措施，因此在节能性方面优于AODV协议。但是AODVjr协议没有在路由过程中采取安全措施，因此不能对路径信息和传送的数据提供安全保障。该文将SRP安全算法应用于AODVjr协议，提出了能够保障路径信息安全的SAODVjr协议，并给出了协议安全性的理论证明。

关 键 词 AODVjr协议； 路由协议； 安全性； 无线传感器网络

中图分类号 TP368 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.z1.029

SRP Based Secured AODVjr Routing Protocol for Wireless Sensor Network

LIANG Zi-lu, XIAHOU Shi-ji, and CHEN Dong-yi

(Mobile Computing Center, University of Electronic Science and Technology of China Chengdu 610054)

Abstract A wireless sensor network (WSN) is a group of spatially distributed sensor nodes that cooperatively monitor the physical or environmental conditions. Routing is an important issue in WSN and routing protocol is responsible for the routing function. AODVjr routing protocol, a simplified version of the widely used Ad hoc on-demand distance vector (AODV) routing protocol, removes the optimization strategies from the original AODV routing protocol such as HELLO message mechanism and route error message broadcasting mechanism; while inherits only the dynamic characteristic from AODV routing protocol. Due to this simplification, AODVjr outperforms AODV routing protocol in energy consumption and thereby is widely used in various WSNs.

Key words AODVjr; routing protocol; security; wireless sensor network

无线传感器网络由大量具有微处理能力的传感器节点组成，涉及传感器技术、嵌入式技术、分布式信息处理技术和无线通信技术。传感器节点采用电池供电，要求一节普通的五号电池能够支持数个月甚至一年以上。因此，无线传感器网络路由需要将节能作为重要的设计指标，以延长网络的生命期。值得注意的是，在无线传感器网络中，路由协议不仅要考虑降低单个节点的能耗，更要关心整个网络的能量消耗问题。

无线自组网按需平面距离矢量协议AODV[1]是一个被广泛采用的传统无线自组网路由协议。如果将其直接应用于无线传感器网络，由于该协议本身所具有的复杂性，将不能满足无线传感器网络低功耗路由的要求。AODVjr协议[2]在考虑了无线节点的有限移动性之后，以最大限度降低节点功耗为目的，对AODV协议进行了简化。AODVjr协议仅保留了AODV协议按需路由的动态特性，而将HELLO消息、路由错误信息、问询序列号等AODV协议为了适应节点移动性提出的优化措施统统省略，对AODV协议进行了最大限度的简化。受益于这样的简化，AODVjr协议在能耗方面极大地优于AODV协议，因此AODVjr协议被广泛应用于各种无线传感器网络。

AODVjr协议最大的问题是没有考虑路由的安全性，不仅数据在传输过程中极有可能被篡改或故意丢弃，路径信息本身也有可能被更改。这必然对网络的健壮性产生不利影响。SRP安全算法是一种端到端的安全机制，它仅在源节点和目的节点处关注安全性，能够有效地节约网络资源，并且不会在

收稿日期： 2009 ↖ 11 ↖ 15
基金项目：中加政府间科技合作基金(2009DFA12100)
作者简介：梁滋璐(1988 ↖)，女，硕士生，主要从事无线自组织网络路由协议方面的研究.

中间节点处增加额外开销。本文用SRP安全算法对AODVjr协议进行安全化，以达到保障路径安全性的目的。若将待传输数据捎带到路由信息中，则可以保障所传输数据的安全性。单纯对传输数据本身安全性的保障可以通过采用相关的加密算法实现，不在本文的讨论范围之内。

1 AODV协议及AODVjr协议

无线自组网按需平面距离矢量协议AODV是一种按需路由的动态协议。与用路由表保存网络路由信息的静态协议不同，它不需要周期性地广播信息更新路由表。当源节点需要向目的节点传送数据时，它才广播一个路由请求(RREQ)启动一个路经寻找过程。因为AODV协议避免了发送周期性的路由更新消息，所以可以降低网络的开销，节约通信带宽；同时，由于不需要采用路由表存储路由信息，AODV协议可以为无线节点节约宝贵的内存资源。AODV协议的特点是引入了数据包序列号(sequence number)和HELLO消息(HELLO message)两种机制。前者保证网络即使处于修复破损链路状态也不会出现路由环路；后者则保证节点能够及时知晓链路的连接状况。当网络规模增加时，AODV协议也能够保证令人满意的网络性能。

AODVjr协议是对AODV协议的简化版本，其编程与调试时间不到AODV协议的一半，资源消耗少，实现起来相对容易得多，但性能却与AODV协议相差无几。所以无线传感器网络多采用AODVjr路由协议，在最大限度保证协议性能的前提下达到节约能源的目的。

为了维持路径的可用性，路径的生命期只有在收到数据包时才进行更新，而发送数据包不进行路径更新。当路径破损时，源节点等待一段时间收不到来自目的节点的消息时，源节点会停止从目的节点接收消息，而开始一次新的路由请求。AODVjr的工作原理如图1所示，通过采用这种端到端的通信策略，HELLO消息机制和路由错误报告机制完全可以省略，网络的开销因此而大大降低。

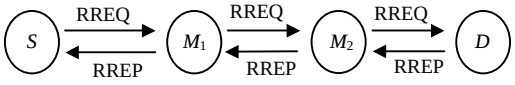

图1 AODVjr协议工作原理

2 SRP安全算法及其改进

AODVjr协议的控制包内不含易变域，使保持其安全化变得相对容易。可以考虑采用一种与ARIN[3]相似的安全算法。ARIN算法采用由一个可靠的第三方提供加密证来保证路由的安全性，整个网络中所有的有效节点都应该知晓该证书供应方的公匙。证书供应方通过带宽外的渠道与每个节点交换钥匙。每个节点在被证书供应方认证之后可以获得一个证书。各个节点都有整个网络所有其他节点的公匙，中间节点就能够验证每个转发的路由包的真实性。但是，公匙加密机制会增加中间节点的开销，随着网络范围的加大，这种算法被认为是不现实的。其次，节点的IP地址并没有得到保护，这是由AODVjr协议本身的性质所决定的，所以将证书与IP地址关联起来也是不合理的。本文采用SRP算法[4]增强AODVjr协议的安全性。

SRP算法是一种端到端的安全算法机制，即仅在源节点和目的节点处关注安全性，中间节点则不予以考虑，这与ARIN算法非常不同。SRP算法有如下假设：

(1) 通信信道为对等的双向信道。

(2) 源节点和目的节点之间存在一个安全联系(SA)。通过事先知晓的通信末端节点的公匙就可以实现这种信任关系。

(3) 两个节点可以通过椭圆曲线Diffie-Hellman[5]算法协商出一个共享的密匙，然后用SA与证实参与交换的节点确实是可以信赖的。

(4) 存在一对共享密匙$K_{S,D}$控制数据朝两个方向流动，从而保证SA的双向性。

(5) 数据链路层提供了可靠的双向传输。

(6) 有媒体访问层地址到IP地址的一对一映射。

(7) 每次传输都会被所有的邻节点正常接收到。

当源节点S发出一个路由请求消息RREQ时，会给该路由请求消息一个问询序列号(query sequence number)和一个随机问询标志(random query identifier)，用来标识该路由请求的标志。然后以源节点IP地址、目的节点IP地址、问询序列号、随机问询标志和共享密匙$K_{S,D}$作为输入计算消息识别码MAC(message authentication code)。

中间节点M_i (i=1,2,…)将自己的IP地址附加到RREQ包中，并对RREQ进行中继，中间节点可以在链路破损时作出反馈，在某些情况下，它们还能提供路由响应，但是考虑到AODVjr协议禁止中间节点对路由请求作出响应，本文也将禁止SRP算法的该项功能。

通常目的节点会多次接收到来自不同中间节点的同一路由请求。这时，SRP规定目的节点保留最

近收到的该路由请求，而将先前接收到的丢弃掉。但是在AODVjr中，根据“最快即最好”原则，目的节点只会对第一个收到的RREQ作出响应。这样可以有效地缩短路由发现时间，并且节约能源和内存。当路由请求到达目的节点D时，目的节点构造出路由响应消息RREP，并以路由请求消息为输入计算出MAC，然后逆着路由请求消息来的路径将路由响应传输给源节点S。源节点会检验该路由响应的有效性，如果是有效的路由响应，则认为可以通过该路径向节点D传输数据。在SRP算法中，路由响应可以通过多条路径传回源节点，但是考虑到AODVjr协议中路由响应只能以单播(unicast)的方式传回源节点，为了配合AODVjr协议的运行原理，本文对SRP协议进行了一定改动。既然目的节点只响应最先收到的RREQ，那么RREP就逆该RREQ来的路径传回源节点S。

3　安全化的AODVjr协议——SAODVjr协议

3.1　基本假设

AODVjr协议在AODV协议基础上进行了大量删减，将HELLO消息、数据包序列号、路径长度、路由错误报告等统统省略，从而极大地节省了网络资源。在没有考虑安全因素的前提下，AODVjr可以表现得与AODV相差无几。但在考虑安全因素时，AODVjr协议由于过于简化，反而不利于安全机制的运行，并且可能导致网络中出现路由环路。基于以上考虑，本文在AODVjr协议中引入问询标志Q_{ID}，源节点同一次发出的所有问询将获得相同的标志，以避免中间节点将同一问询转发多次，或目的节点对同一问询作出多次响应。同时，由于SRP与AODV在路由机制上略有差异，本文对SRP算法也进行了一些适用于AODVjr协议的改良，这在前一部分中已经提到。

综上所述，本文将SAODVjr协议的基本假设总结如下：

(1) 通信信道为对等的双向信道，源节点和目的节点之间存在一个安全联系(SA)和一对共享的钥匙$K_{S,D}$控制数据朝两个方向流动，从而保证SA的双向性。

(2) 在AODVjr协议基础上，引入问询标志Q_{ID}参数。

(3) 目的节点只响应最先收到的路由请求，对于之后收到的同一请求不予响应。路由响应以单播的方式逆路由请求的路径传回源节点。

(4) 仅目的节点响应路由请求，中间节点不得响应路由请求。

(5) 数据链路层提供了可靠的双向传输，每一次传输都会被所有的邻节点正常接收到。

(6) 有媒体访问层地址到IP地址的一对一映射。

3.2　路由请求RREQ

源节点在每一次发起RREQ时激发一个32 bit的随机问询标志Q_{ID}。中间节点通过该标志来识别路由请求。本文采用一个安全伪随机数产生器[6]来产生Q_{ID}，该伪随机数产生器的输出与真正的随机数在统计学意义上并没有差别。一个计算能力有限的坏节点是没有能力预见其输出的。

MAC域长96 bit。以目的节点地址(dest)、源节点地址(scr)和共享的钥匙$K_{S,D}$作为单向散列函数(如SHA-1或MD5[7])的输入，通过计算其输出，可以获得相应的MAC码：

$$S \rightsquigarrow \mathrm{MAC}{:}H\{\mathrm{dest},\mathrm{scr},K_{S,D}\} \tag{1}$$

当源节点需要与另一节点进行通信而又没有通往该节点的路径信息时，源节点便通过向邻节点广播一个路由请求消息RREQ发起一个路径寻找过程：

$$S \rightsquigarrow \mathrm{brdcast}{:}[\mathrm{dest},\mathrm{scr},Q_{\mathrm{ID}},\mathrm{MAC}] \tag{2}$$

路由请求RREQ的格式如图2所示。

类型	D	G	保留字
目的节点IP地址			
源节点IP地址			
中间节点IP地址			
问询标识Q_{ID}			
SRP消息识别码MAC			

图2　SAODVjr的RREQ包格式

其中类型取值为1，表示该包为路由请求消息；D的值设为1，表示中间节点不得响应该RREQ；G的值也设为1，表示通信信道为双向；保留字默认为0；中间节点IP地址域用于存放该RREQ消息到达目的节点所经过路径上所有中间节点的IP地址。

3.2　RREQ的中继

中间节点对RREQ进行中继。假设中间节点M_i从邻节点处接收到RREQ，M_i首先将Q_{ID}提取出来，如果该Q_{ID}与节点问询表(query table)的某个入口相符合，则舍弃接收到的RREQ；否则，M_1继续提取出源节点S和目的节点D的地址，与Q_{ID}一起在问询表中创建一个入口。然后将自己的IP地址加入到RREQ的中间节点IP地址域中，并将该RREQ广播出去：

$$M_i \rightsquigarrow \mathrm{brdcast}{:}[\mathrm{destr},\mathrm{scr},Q_{\mathrm{ID}},\mathrm{MAC},(\mathrm{addr}M_1,\mathrm{addr}M_2,\cdots,\mathrm{addr}M_{i-1},\mathrm{addr}M_i)](i=1,2,\cdots) \tag{3}$$

路径上的每个节点都重复这样的工作，检查收到的RREQ是否已经被处理。若没有，则提取出目的节点IP地址、源节点IP地址和问询标志Q_{ID}在问询表中创建一个新的入口。将自己的IP地址附加到RREQ中的相关域，然后将该RREQ广播出去，直到该RREQ到达目的节点为止。

中间节点还将检测从邻节点接收问询的频率，并根据这个频率给邻节点划分优先级。通常最高优先级会分配给频率最低的节点，反之亦然。坏节点的邻节点会检测到极高的问询接收频率，如果是这样，邻节点们会更新它们相应的优先级。低优先级的问询得不到响应，就等于已经被丢弃。这样，坏节点就达不到消耗网络资源、降低网络性能的目的。

3.4 路由响应RREP

当目的节点D接收到RREQ时，会首先检验该RREQ是否来自于一个与之存在SA关系的节点。然后，D提取出该RREQ的Q_{ID}，以判断是否已经接收过与该RREQ相同的请求。若已经接收过，则丢弃该包不作响应；否则，提取出目的节点IP地址、源节点IP地址和问询标志Q_{ID}为单向散列函数的输入，如果输出与该RREQ中的消息识别码一致，则认为该RREQ是有效的，其真实性也得到证明。

在证实该RREQ的有效性之后，目的节点D开始构造相应的路由响应RREP。D首先将RREQ中的目的节点地址、源节点地址、中间节点IP地址和问询标志Q_{ID}复制到相应区域，然后以目的节点地址、源节点地址、中间节点IP地址和共享密匙$K_{S,D}$作为单向散列函数的输入计算消息识别码MAC。该MAC码可以向源节点S证明目的节点D确实接收到了其发出的路由请求：

$$D \rightarrow \text{MAC}:H\{\text{dest,scr,}(\text{addr}M_1,\text{addr}M_2,\cdots,\text{addr}M_{i-1},\text{addr}M_i),K_{S,D}\} \quad (4)$$

路由响应RREP的格式如图3所示。

类型	A	节点数	保留字
目的节点IP地址			
源节点IP地址			
中间节点IP地址			
问询标识Q_{ID}			
SRP消息识别码MAC			

图3 SAODVjr的RREP包格式

其中类型取值为2，表示该包为路由响应；A取值为0，表示不需要向目的节点确认RREP的接收；节点数表示路径上所有中间节点的数量：

$$D \rightarrow \text{unicast:[dest,scr,}(\text{addr}M_1,\text{addr}M_2,\cdots,\text{addr}M_{i-1},\text{addr}M_i),Q_{ID},\text{MAC}] \quad (5)$$

目的节点将RREP逆着该RREQ来的路径传输回源节点。

3.5 检验RREP的有效性

当接收到来自目的节点D的路由响应时，源节点S首先检查RREP中源节点地址、目的节点地址和问询标志Q_{ID}，如果与当前最迫切的问询不一致，则将该RREP丢弃；否则，源节点提取出目的节点地址、源节点地址、中间节点IP地址与$K_{S,D}$一起作为单向散列函数的输入计算消息识别码MAC，若结果与RREP中的MAC码相符，则S认为路由请求确实完好无损地到达了目的节点D。而且，路由响应能够沿着该路径被源节点S成功接收，说明路径信息在RREQ传输的过程中没有被破坏，该连接信息是真实可信的。

4 协议的正确性论证

为了论证协议的正确性，本文用文献[8]中的方法对协议的安全性进行了验证。

假设X和Y是公式，P和Q是原语，K是共享密匙，C是一个陈述。遵循文献[9]中规定的符号体系：

- $P \triangleleft X$：P被告知X。
- $X \ni P$：P拥有或者有能力拥有X。
- $P|\sim X$：P说了X。
- $P|\equiv P \overset{K}{\leftrightarrow} Q$：$P$相信或有资格相信$P$和$Q$可以通过共享密钥$K$进行通信，且这个$K$是好的，即不会被$P$和$Q$不信任的原语知道。
- $P|\equiv \#(P)$：P相信它能确认一个消息不是源自它自己。
- $P|\equiv C$：P相信或有资格相信陈述C成立。
- (X, Y)：两个公式的联合。是一个带有联合性和交换性的集合。
- $*X$：公式的“不源于此”性质。如果P被告知X，则P能够辨别出自己之前没有说过X。
- $H(X)$：X的单向散列函数值。
- 分隔两个陈述或陈述的联合的水平线表示线上面的陈述能够推出线下面的陈述。如 $\dfrac{P \triangleleft (X,Y)}{P \triangleleft X}$ 表示，由P被告知(X, Y)可以推出P被告知X。

将协议抽象成路由请求RREQ和路由响应RREP在一个公共信道上的传播，如图4所示。路径上一系列的中间节点都有被攻击的可能。

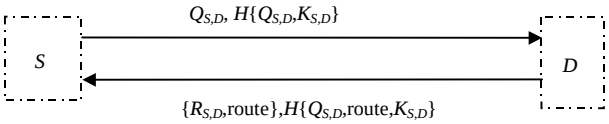

图4 抽象化的SAODVjr协议

$Q_{S,D}$和$R_{S,D}$分别代表路由请求RREQ和路由响应RREP；H代表单向散列函数，$H\{\}$表示请求消息识别码MAC的过程。与$Q_{S,D}$有关的域包括问询标志Q_{ID}以及源节点和目的节点的地址。

下面对协议的安全性进行论证：

(1) $K_{S,D}$ S，$S|\equiv S \overset{K_{S,D}}{\leftrightarrow} D$，$Q_{\mathrm{ID}}$ S

源节点S拥有共享密匙$K_{S,D}$，且相信该密匙可以用于自己和目的节点D相互证明身份。源节点为RREQ分配一个独特的问询标志Q_{ID}用于识别该问询。

(2) $K_{S,D}$ D，$D|\equiv S \overset{K_{S,D}}{\leftrightarrow} D$，$D \lhd Q_{\mathrm{ID}}$，$D|\equiv S|\sim Q_{\mathrm{ID}}$。

目的节点D同样拥有共享密匙$K_{S,D}$，并相信自己和源节点S可以使用该密匙进行通信。D会被告知该RREQ的Q_{ID}，并且相信源节点说了Q_{ID}。此外，S与D都相信它们能够分别识别路由请求$Q_{S,D}$和路由响应$R_{S,D}$。

(3) $S|\equiv(R_{S,D}, H\{R_{S,D},K_{S,D}\})$，$D|\equiv(Q_{S,D}, H\{Q_{S,D},K_{S,D}\})$。

源节点S相信它能确认伪造的$R_{S,D}$和MAC码不是源于自己；同理，目的节点D相信它能确认伪造的$Q_{S,D}$和MAC码不是源于自己。

(4) $\dfrac{D \lhd *(Q_{S,D},H(Q_{S,D}, K_{S,D}))}{D \lhd (Q_{S,D},H(Q_{S,D}, K_{S,D}))}$，以及 $\dfrac{D \lhd (Q_{S,D},H(Q_{S,D}, K_{S,D}))}{(Q_{S,D},H(Q_{S,D}, K_{S,D}))\ D}$。

根据“不源于此”性质，当D收到一个包的时候，它会辨别自己是否之前已经传播过该包。

(5) $\dfrac{(Q_{S,D},H(Q_{S,D}, K_{S,D}))\ D}{(Q_{S,D}\ D,H(Q_{S,D}, K_{S,D}))\ D, Q_{ID}\ D}$。

同样，可以推出目的节点D拥有$Q_{S,D}$剩下的域中的内容。

从步骤(1)～(5)可以得出如下结论：

$D \lhd H\{Q_{S,D},K_{S,D}\}$，$(Q_{S,D},K_{S,D})$ D，$D|\equiv S \overset{K_{S,D}}{\leftrightarrow} D$

(6) $\dfrac{D \lhd (Q_{S,D},H(Q_{S,D}, K_{S,D})),D|\equiv S \overset{K_{S,D}}{\leftrightarrow} D}{D|\equiv S|\sim Q_{S,D},D|\equiv S|\sim H\{Q_{S,D}, K_{S,D}}$。

证实了路由请求和消息识别码均来自源节点。而且，之前就假设两个原语不会泄露共享秘匙，所以源节点不会泄露秘匙。

(7) $\dfrac{(Q_{S,D},H(R_{S,D}, K_{S,D}))\ S}{(R_{S,D}\ S,H(Q_{S,D}, K_{S,D}))\ S}$，以及 $\dfrac{Q_{ID},\mathrm{route}\ S}{R_{ID}\ S}$。

根据“不源于此”性质，可知：

$S \lhd H\{R_{S,D},K_{S,D}\}$，并且$(R_{S,D},K_{S,D})$ D，$S|\equiv S \overset{K_{S,D}}{\leftrightarrow} D$

(8) $\dfrac{S \lhd (Q_{S,D},H(Q_{S,D}, K_{S,D})),S|\equiv \overset{K_{S,D}}{\leftrightarrow} D}{S|\equiv D|\sim R_{S,D},S|\equiv D|\sim H\{Q_{S,D}, K_{S,D}\}}$。

据此，源节点S相信整个路由响应来自于目的节点D，并且已经建立起通往D的路径。假设没有串通起来的坏节点，路由响应只可能逆着路由请求到达的路径抵达源节点。同时，既然路由响应能够逆该路径到达源节点，也就说明路由响应的内容在其构造之前没有被更改过。因此，路由响应顺利到达源节点S说明相应的连接信息是正确的，即证明SAODVjr协议能够保障路径的安全性。

5 结 论

本文在AODVjr路由协议基础上提出了一种基于SRP安全算法的能够保障路径安全性的路由协议。理论证明其能够达到保证路径安全的目的。但该协议并不能保证传输数据的安全性。此外，该协议也没有考虑能耗和网络开销。因此，对该协议的优化可以从以上两个方面入手。总的来说，SAODVjr协议能够为整个无线传感器网络提供安全的路由。

参 考 文 献

[1] CHARLES E P, ELIZABETH M B. Ad hoc on-demand distance vector (AODV) routing[S]. IETF RFC 3561.

[2] IAN D C, LUKE K B. AODVjr, AODV simplified[J]. Mobile Computing and Communications Review, 2002, 6(3): 100-101.

[3] KIMAYA S, BRIGET D, BRIAN N L, et al. A secure routing protocol for Ad hoc network[C]//Proceedings of the 10th IEEE International Conference on Network Protocols. [S.l]: IEEE, 2002.

[4] PAPADIMITRATOS P, HAAS Z J. Secure routing for mobile Ad hoc network[C]//Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002). San Antonio, TX: [s.n.], 2002.

[5] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[6] MENEZES A, VAN OORSCHOT P, VANSTONE S. Handbook of applied cryptography[M]. [S.l.]: CRC Press, 2001.

[7] RIVEST R. The MD5 message-digest algorithm[S]. RFC 1321, 1992.

[8] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[C]//Proceedings of the 12th ACM Symposium on Operating System Principles. Arizona: ACM, 1989.

[9] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]//Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 1990.

编 辑 税 红

(上接第102页)

参 考 文 献

[1] DELLER J R, PROAKIS J G, HANSEN J H L. Discrete-time processing of speech signals[M]. New York: Maxell McMillan, 1993.

[2] FORT A, ISMAELLI A, MANFREDI C, et al. Parametric and non-parametric estimation of speech formants: application to infant cry[J]. Med Eng Phys, 1996, 18(8): 677-691.

[3] PARSONS T. Voice and speech processing[M]. New York: McGraw Hill, 1986.

[4] RABINER R L, SCHAFER R W. Digital processing of speech signals. Englewood Cliffs[M]. New Jersey: Prentice-Hall, 1978.

[5] BENJAMIN K. Spectral analysis and discrimination by zero-crossings[C]//Proceedings of the Institute of Electrical and Electronics Engineers. [S.l.]: [s.n.], 1986: 1477-1493.

[6] CURTIS R. The computer music tutorial[M]. Cambridge: MIT Press, 1996.

[7] DE CHEVEIGNE A, YIN H K. A fundamental frequency estimator for speech and music[J]. Journal of the Acoustical Society of America, 2002, 111(4): 1917-1930.

[8] EARGLE J M. Music, sound and technology[M]. Toronto: Van Nostrand Reinhold, 1995.

编 辑 税 红