多对一加密认证方案在视频会议中的应用

刘秀燕 魏振钢 林喜军 邢 静

(中国海洋大学信息科学与工程学院 青岛 266100)

摘 要 针对视频会议中存在的安全隐患问题及产生的原因,提出了在视频会议中使用多对一加密认证方案加密会话密钥的方法,该方法使用二次加密的方法保证了会话密钥的安全性,分析证明了该方案能有效解决会话密钥泄露造成的传输数据被非法人员窃取利用的问题,并减轻了密钥管理的负担。

关键词 视频会议,多对一,加密认证,安全性

中图法分类号 TP39 **文献标识码** A

Application of Many-to-one Encryption and Authentication Scheme in Video Conference

LIU Xiu-yan WEI Zhen-gang LIN Xi-jun XING Jing

(College of Information Science and Engineering, Ocean University of China, Qingdao 266100, China)

Abstract According to the existing safety problems and the causes in video conference, this paper proposes the scheme that using many-to-one encryption and authentication scheme to encrypt the session key. The scheme using secondary encryption method to ensure the security of the session key in conference. Analysis shows that the scheme can effectively solve the session key transmission data is caused by leakage illegal personnel stealing utilization, and reduce the burden of key management.

Keywords Video conferencing, Many-to-one, Encryption and authentication, Security

1 引言

随着计算机技术、网络技术和多媒体通信技术的发展,视频会议的应用越来越频繁,如远程监控、远程教学、远程医疗诊断、政治、经济、军事等各方面;视频会议利用计算机强大的信息处理能力逐渐取代了传统会议模式,成为人们获取各种信息的重要手段,是一种经济、方便、快速、高效、便捷的交流工具。然而,在视频会议中,经常会出现无关人员擅自闯入会议中进行复制资料、更改会议机密信息,破坏会议秩序,因此人们希望在相互交流的时候不受到外界的干扰,信息不被外泄。如果视频会议过程中出现了安全问题,那就意味着恶意的攻击者不仅可以看到视频会议内容,而且会议所有人员的信息都将被窃取、篡改,这样可能会给使用会议系统的企业、政府部门、事业单位等造成严重的损失和危害。因此,视频会议安全问题日益突出,如何保证信息的安全性迫在眉睫。一般有两种方法实现加密,第一种方法:使用对称加密算法如数据加密标准 DES(Data Encryption Standard)算法,发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。此方法的缺点是服务器需要保存大量的密钥,密钥的数目难于管理,如果合法发送者数目较大,那么找到一个合适的解密密钥也是个费时的操作,因此该方法有一定的局限性。第二种方法:使用非对称加密算法如因特网加密和认证体系 RSA (Rivest Shamir Adlemen)算法,用公开密钥对数据加密,只能用对应的私有密钥进行解密,所有合法发送者用不同的签名来验证身份,该方案使得服务器需要保存太多的密钥来验证签名,接收者仍需保存大量身份认证,并没有减少接收者的工作量和存储空间,而且加密和解密花费时间长、速度慢。还有很多基于证书的公钥方案[1],服务器不需要保存任意的密钥来认证身份,但是如何在基于身份的密码系统中撤销合法发送者身份也是一个难题。

因此,针对目前视频会议安全保密系统存在的问题,我们提出了多对一加密认证安全机制,每个发送者之间的密钥互不相同,在接收到加密密钥之后,发送者才能发送密文给接收者。我们引入密钥生成中心(KGC, Key Generation Center)来生成加密密钥,分担接收者分配加密密钥的繁重工作,因此接收者的密钥管理变得更简单,接收者使用唯一的密钥解密和认证接收到的密文,从而保证了数据传输的安全性。

2 视频会议系统及其安全机制

所谓视频会议系统是指利用计算机技术和通信设备通过传输信道在两点或多个地点之间建立可视通信,并通过传输线路及多媒体设备,将声音、影像及文件资料互传,实现数据、语音及图像即时互动的沟通、交流的一种会议形式[2]。视频会议系统是一种虚拟化的会议应用系统,其基本功能是利用网络通信技术满足人们跨越空间界限,支持远距离进行实时信息交流与共享、开展协同工作、实现异地"面谈"需求。

本文受国家自然科学基金资助项目(41276085),青岛市科技计划基础研究项目(11-2-4-1-(6)-JCH)资助。

刘秀燕(1987—),女,硕士生,主要研究方向为信息安全、密码学、软件工程与智能信息系统、数据挖掘与数据仓库等,E-mail:liuxiuyan_ok@163.com;魏振钢(1962—),男,教授,主要研究方向为软件工程与智能系统等;林喜军(1977—),男,博士生,讲师,主要研究方向为信息安全、密码学;邢 静(1988—),女,硕士生,主要研究方向为软件工程与智能系统、数据挖掘与数据仓库、信息安全等。

目前视频会议系统被广泛应用到涉及私人信息、商业秘密、军事情报及国家机密等的各个领域，因此视频会议系统的安全保密问题成为一个重要的问题。视频会议安全系统应用于通信双方两个终端或者一个终端和一个主会场的点对点连接[3,4]。视频会议系统安全保密方法，如图 1 所示。

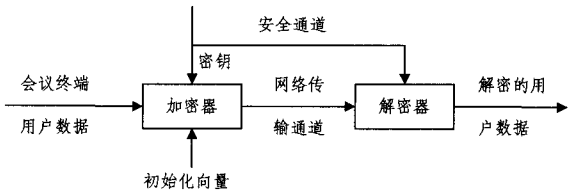

图 1　视频会议系统安全保密方法

视频会议安全保密结构的主要组成是加密模块和解密模块，加密模块主要是对各分会场及主会场发送的媒体数据进行加密，解密模块的作用是对接收到的数据进行解密还原出用户数据。密钥的生成和管理是加密模块和解密模块的核心，保证密钥的安全是视频会议系统的关键。ITU-T 指定的标准中并没有给密钥的产生及管理作较多的规定，因此，对加密算法的研究和设计就成为当前信息安全领域的一个热点，开发者可以根据自己的思路和需要对视频会议安全保密系统进行设计，使用新方法更有效地管理密钥。

目前视频会议系统中常用的加密算法是：非对称加密算法 RSA 和对称加密算法 DES。为了达到视频会议中的语音、视频信息等保密的目的，首先需要提供一条私有的控制信道，其功能是传递密钥信息。现有的视频会议系统密码体系，各分会场与主会场使用相同的密钥，当有终端加入会议或提前离开会议时，为防止密钥泄露造成机密信息被公开需要更新密钥，重新更换通信密钥会浪费很多时间和资源，而且在传送过程中容易泄露，针对以上存在的问题提出了加密会话密钥的多对一加密认证方案。

3　多对一加密认证算法实现过程

3.1　视频会议的原理

所谓多对一加密认证算法，顾名思义就是指一个接收者服务于多个发送者，相比于发送者，服务器数量是很少的，每一台服务器可以接受来自上百万发送者的信息。该算法的优点有：每一个合法的发送者都拥有一个独立的密钥来构造密文，非常容易实现撤销发送者发送的信息，且不会影响服务器和其他发送者的计算复杂性。衡量一个加密算法的最重要的指标就是安全性，任何加密算法都应该首先满足安全性要求，本文采用多对一加密认证算法对视频会议中的每个会话密钥进行加密，以保证传输安全保密。

直接使用商定的密钥对数据信息进行加密存在密钥泄露的风险，致使会议内容被窃取。下面阐述视频会议中使用二次加密的方法保证传送数据的安全，首先传送加密的会话密钥，然后双方使用该密钥对数据信息加解密。使用二次加密方法的视频会议系统安全如图 2 所示：

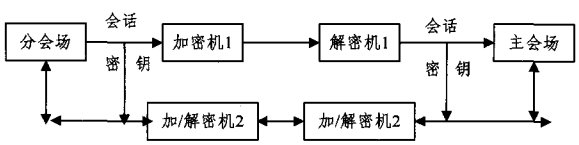

图 2　二次加密的视频会议系统安全保密框图

下面进行安全性分析：一次加密时密文＝加密算法(明文，密钥)，密文的安全性依赖于密钥和加密算法的安全性，如果使用国际标准的加密算法，那么密文的安全则只依赖于密钥的安全性。如果使用二次加密，密文＝加密算法 2(加密算法 1(明文，密钥 1)，密钥 2)，密文的安全性取决于加密算法 1、密钥 1、加密算法 2、密钥 2，攻击者需要同时得到 4 项信息才能获取明文，安全性得到了很大程度的提高。

会议开始时，要加入会议的分会场需要与主会场建立连接，在发送申请加入会议“通信帧”的同时向主会场发送一个使用多对一加密认证算法加密的会话密钥。主会场解密出此会话密钥并用此密钥加密回复信息，若同意此分会场加入视频会议，连接建立。在进行视频会议通信时此分会场和主会场使用该会话密钥加密数据。其他分会场加入视频会议过程也是如此，各分会场通过主会场建立连接，主会场控制会议流程及各分会场的交互。主会场和分会场建立连接的过程如图 3 所示：

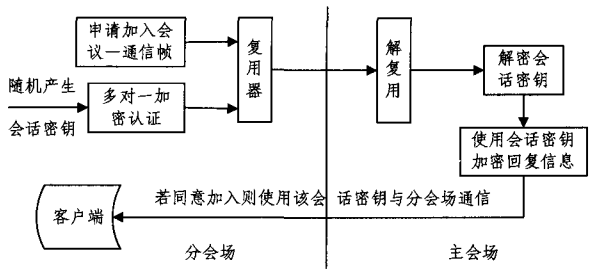

图 3　分会场与主会场建立连接过程

多对一加密认证方案是使用椭圆曲线上的双线性映射作为工具，利用基于双线性配对的密码系统的快速原型库(PBC，Pairing-Based Cryptography)实现。PBC 提供了双线性映射循环群的抽象接口，使程序和数学细节分离出来。下面将结合 PBC 库和多对一加密认证算法方案详细阐述加密解密实现过程[5-7]。

3.2　加密认证算法的实现过程

先给出多对一加密认证方案中的 6 个函数参数变量的名称：安全参数 K、系统参数 $Params$、系统主密钥 MK、发送者身份 ID_A、接收者身份 ID_S、接收者私钥 SK_S、接收者信息 $Info_s$、合法发送者的加密密钥 $EK_{A,S}$、明文 M、密文 C、非法密文错误信息 $Error\text{-}Info_s$，函数列表如表 1 所列。

表 1　函数列表

函数名称	参数列表	返回值
Setup	K	Params MK
Private-Key-Extract	Params ID_S	SK_S
Information-Extract	Params SK_S ID_S	$Info_s$
Encryption-Key-Generation	K MK ID_A ID_S $Info_s$	$EK_{A,S}$
Encrypt	Params $EK_{A,S}$ M	C
Decrypt	Params SK_S ID_A ID_S M	M or Error-$Info_s$

1) *Setup*：该函数的主要功能是初始化参数，为下面的加密解密过程做准备。步骤为：第一步：密钥生成中心 KGC (Key Generation Center)产生 K，其中 K 为 512 位，是 P 阶素数群$(G,+)$和同阶群(F,g)，群 G 中生成元 P，其中 $P\in G$，$element_random(P)$函数产生随机数；第二步：给出双线性映射 $e:G\times G\rightarrow F$，选取 $s\in_U Z_P^*$，$element_random(s)$生随机数 s；第三步：设 $P_0=sP$，$Params=(G,F,e,n,P,P_0,SHA1)$，$element_mul_zn(P_0,P,s)$计算 $P_0=sP$；第四步：得出 $MK=s$，其中 $SHA1$ 是 SHA 系列单项散列函数。

2) *Private-Key-Extract*：该算法输入 *Params* 和 ID_S，输出 SK_S，执行步骤为：第一步：随机选择两个参数 $a,b\in_U Z_p^*$，产生随机数 a,b 的过程 *element_random*(a)，*element_random*(b)；第二步：输出 SK_S，即 $SK_S=(a,b)$；

3) *Information-Extract*：该算法输入 *Params*、ID_S 和 SK_S，输出 $Info_s$，为下一步产生相应的合法发送者的加密密钥做准备，执行步骤为：第一步：执行 $SK_S=(a,b)$ 得到 SK_S；第二步：输出 $Info_s=e(aQ_s,bP)$，其中 $Q_S=SHA1(ID_S)$ 的具体运算过程为：假设 ID_S 用"*AB*"表示，使用哈希运算求得 Q_s，*element_from_hash*(Q_s,"*AB*",2)；

计算 $t1=aQ_s$：*element_mul_zn*($t1,Q_s,a$)；

计算 $t2=bP$：*element_mul_zn*($t2,P,b$)；

最后计算 $Info=e(t1,t2)=e(aQ_s,bP)$，即 *element_pairing*($Info,t1,t2$)；

4) *Encryption-Key-Generation*：该算法输入 *Params*、主密钥 $MK=s$、$Info_s$、ID_A、ID_S，输出 $EK_{A,S}$，执行步骤为：第一步：计算 $\gamma=SHA1(Info_s,ID_A)$；计算过程：先把 $Info_s$ 转换成字节类型并存入数组 *temp* 中，即 $t=$ *element_to_bytes*(*temp*,$Info_s$)；然后将数组 *temp* 和 ID_A 进行哈希运算，即实现 $Info_s$ 和 ID_A 的哈希：*element_from_hash*($t3$,*temp*,$t+7$)；第二步：求出 EK_1 和 EK_2，其中 $EK_1=\frac{1}{SHA1(ID_A)+s}Q_s$、$EK_2=Info_s^{\gamma}$；

计算 EK_1 的过程：首先使用"*ABCDEFG*"这 7 个字母表示 ID_A，计算出 $t7=SHA1(ID_A)$，即 *element_from_hash*($t7$,"*ABCDEFG*",7)；然后计算 $t4=t7+s=SHA1(ID_A)+s$：*element_add*($t4,t7,s$)，计算 $t4$ 的逆转 $1/t4$，即 $t4=1/t4=1/(SHA1(ID_A)+s)$，*element_invert*($t4,t4$)，最后计算 EK_1，$EK_1=Q_st4=Q_s/(SHA1(ID_A)+s)$，*element_mul_zn*($EK1,Q_s,t4$)；

计算 EK_2 的过程：$EK_2=Info_s\wedge t3$，即

element_pow_zn($EK2,Info_s,t3$)

第三步：输出 $EK_{A,S}$，即 $EK_{A,S}=(EK_1,EK_2)$；

5) *Encrypt*：该函数先接收 $EK_{A,S}$，然后输入 *Params*、$EK_{A,S}$、$M\in\varepsilon$，其中 M 为明文、$\varepsilon=\{0,1\}^n$，产生密文的步骤如下：第一步：随机选择 $r_1\in_U Z_P^*$；在环 $Z_r=_U Z_P^*$ 上随机选取 r_1：*element_random*($r1$)；第二步：计算 $c=r_1P$，$r=SHA1(c,M)$，$u=(r+r_1)EK_1$ 和 $v=M\oplus SHA1(EK_2^r)$；

首先，计算 $c=r_1P$：*element_mul_zn*(c,P,r_1)，然后计算 $r=SHA1(c,M)$：将 c 和明文 M 转换为字节型存入数组 tp，然后对 tp 进行哈希运算，实现 c 和 M 的哈希：

element_from_hash($r,tp,n+strlen(M)$)；

计算 $u=(r+r_1)EK_1$：先计算 $t5=r+r_1$：

element_add($t5,r,r_1$)，然后计算 $u=t5EK_1$：

element_mul_zn($u,EK_1,t5$)；计算 $v=M\oplus SHA1(EK_2^r)$：首先计算 $t6=EK_2\wedge r$ *element_pow_zn*($t6,EK_2,r$)；

然后将 $t6$ 与明文 M 进行按位异或运算：

```
for(int i=0;i<strlen(M);i++){
v[i]=M[i]^t6[i];
cout<<v[i]<<"";
}
```

第三步，输出密文 $C=(c,u,v)$，这样就完成了整个加密过程；

6) *Decrypt*：该算法输入 *Params*、SK_S、ID_A、ID_S、$C=(c,u,v)$，在接收到密文 $C=(c,u,v)$ 后，接收者解密的过程为：

第一步：用 $SK_S=(a,b)$ 计算 $Q_s=SHA1(ID_S)$ 和 $\gamma=SHA1(Info_s,ID_A)$；

第二步：计算 $\alpha=\frac{e(u,ab\gamma(SHA1(ID_A)P+P_0))}{e(c,ab\gamma Q_s)}$；

第三步：计算 $M'=v\oplus SHA1(\alpha)$，判断 α 值，如果 $\alpha=Info_s^{\gamma SHA1(c,M')}$，那么接收者是合法的，可以接收明文 M'，否则输出不合法的密文的错误信息，记为 *Error-Info*$_s$；以上解密过程的正确性很容易得到验证，验证过程如下：

$$\begin{aligned}\alpha&=\frac{e(u,ab\gamma(SHA1(ID_A)P+P_0))}{e(c,ab\gamma Q_s)}\\&=\frac{e((r+r_1)EK_1,ab\gamma(SHA1(ID_A)P+P_0))}{e(r_1P,ab\gamma Q_s)}\\&=e(Q_s,P)^{rab\gamma}\\&=Info_s^{r}\\&=EK_2^r\end{aligned}$$

在接收到合法发送者的密文之前，可以再重新计算 $Info_s=e(aQ_s,bP)$。

注：当使用 *SHA*1 处理身份 *ID* 时，处理完毕后要转换成群 G 中的元素；当使用 *SHA*1 计算 γ 时，要将 *SHA*1 的输出结果截取为 $K-1$ 位，以保证 $\gamma\in Z_p^*$；当使用 *SHA*1 计算 α 时，要将 *SHA*1 的输出结果截取为与 v 相同的位数，以保证两者可以进行异或运算。

根据多对一加密认证算法的描述及视频会议的通信流程，下面给出视频会议加密解密具体的流程，如图 4 所示。

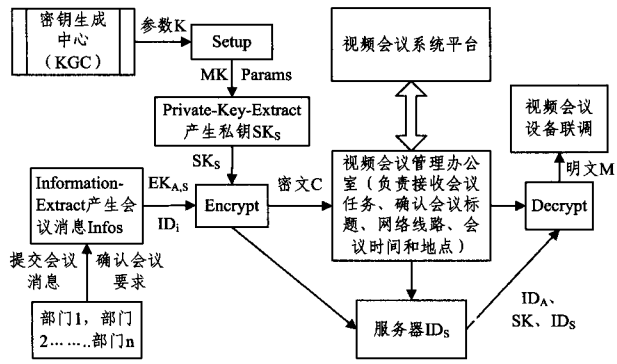

图 4　视频会议加密解密过程

首先，密钥生成中心 KGC 生成系统参数，*Setup* 函数为加密过程做准备工作，以启动加密解密函数，各部门代表分会场，分别向主会场建立连接并提交会议的消息、确认会议的要求，然后使用多对一加密算法将这些消息封装起来，将明文加密为密文，各分会场的终端设备分别解密出明文，视频会议系统平台为各个分会场提供了互相通信的共享平台。多对一加密认证算法的关键步骤是产生加密密钥和解密密钥，产生加密密钥并用其加密的过程如下：产生系统参数($Params,MK$)$=Setup(k)$，为分会场分配身份信息记为 ID_A，产生加密密钥 $EKA,S=Encryption-key-Extract(params,M_k,Info_s,ID_A,ID_S)$，使用 ID_A 和 $EK_{A,S}$ 对会话密钥 M 进行加密

$C=Encrypt(Params,EK_{A,S},M)$。

主会场接收到密文 C 后，产生解密密钥并使用解密算法进行解密的过程如下：主会场身份信息记为 ID_S，产生系统参数和主密钥($Params,MK$)$=Setup(k)$，主会场产生解密密钥 $SK_S=Private-key-Extract(Params,ID_S)$，使用解密密钥对密文进行解密 $M=Decrypt(Params,SK_S,ID_A,ID_S,C)$ 只有

当密文格式正确且是合法用户发送的信息时，主会场才能成功解密出会话密钥。

与传统加密算法相比，多对一加密算法的多个发送者共享一台服务器上的密钥来解密，服务器密钥存储量远远少于发送者的数量，也就是说仅仅使用唯一的密钥可以对所有的发送者的密文进行解密和认证，当合法发送者数目非常大时，就可以避免接收者保存大量认证密钥和发送者名单，因此大大减少了接收者的计算时间和存储空间，节省了系统的开销，密钥的管理也更简单，减轻了其负担，服务器只需要保存主密钥就能解密根据用户身份加密后的密文。

视频会议的安全需求主要体现在[8,9]：身份认证、数据完整性、私密性、不可抵赖性。多对一加密认证算法使用了用户的身份信息产生加密密钥，只有合法用户传送的会话密钥才能被主会场正确解密；数据完整性：使用二次加密保证了会话密钥的安全，两个端点之间进行通信的有效数据不被损坏或篡改，数据完整性得到保证；私密性：即使传送的数据被图谋不轨的人截获，在不知道解密算法和密钥的情况下仍然无法获取有效信息。不可抵赖性：由于多对一加密认证算法的加解密过程是基于身份认证的，防止了发送方和接收方抵赖其所传输的数据。

3.3 算法安全性证明

首先假设存在一个算法 δ 可以伪造密文，则构造算法 β 可以攻破该方案[10-13]，预先选取散列函数 $SHA1$，发送者身份和接收者身份组成序列对 (ID_A, ID_S)，将该问题的参数 (G, F, P, xP, yP, zP, e) 和 $T \in F$ 发送给 β，如果 $e(P,P)^{xyz}=T$，则返回值为 1，否则返回值为 0，算法 δ 作为子程序被算法 β 调用，证明过程如下：δ 发送两个等长的消息 $M0, M1$ 以及身份给 β 作为挑战，如果 ID_i 已经被分配，β 失败，否则，β 做如下计算：若 ID_i^* 没有被分配，则令 $ID_i^*=ID_A^*$，随机选取 $\beta \in \{0,1\}$ 和 $r_1 \in Z_P^*$，(r_1P, M_β) 没有在 $SHA1$ 查询中被查询；通过在 $SHA1\text{-}list$ 中计算 $SHA1(ID_I)$ 获得 θ，通过输入 ID_i 调用 $Information\text{-}Extract$ 得到 $Info_i$，然后计算 $\gamma=SHA1(Info_I, ID_A^*)$、$c^*=r_1P$、$v^*=M_\beta \oplus H(T^{\theta\gamma})$ 和 $u^*=\frac{1}{H_1(ID_A^*)+s}(\theta zP+r_1\theta P)$，最后输出 $C^*=(c^*, u^*, v^*)$ 作为挑战密文。通过推理验证可得到 $u^*=(z+r_1)EK_1$：

$$
\begin{aligned}
u^* &= \frac{1}{H_1(ID_A^*)+s}(\theta zP+r_1\theta P)\\
&= \frac{z+r_1}{H_1(ID_A^*)+s}Q_i\\
&= (z+r_1)EK_1
\end{aligned}
$$

并且可得到：

$$
\begin{aligned}
v^* &= M_\beta \oplus H(T^{\theta\gamma})\\
&= M_\beta \oplus H(\hat{e}(xP, yP)^{\theta yz})\\
&= M_\beta \oplus H(Info_I^{xz})\\
&= M_\beta \oplus H(EK_2^z)
\end{aligned}
$$

$EK_{A,I}=(EK_1, EK_2)$ 作为回应 (ID_A^*, ID_I) 的加密密钥，并且我们隐含地定义 $z=H_2(c^*, M_\beta)$，如果 $T=\hat{e}(P,P)^{xyz}$，那么 C^* 是合法的明文。

结束语 本文针对视频会议安全保密系统中密钥容易泄露的问题，在现有加密解密算法的基础上提出了使用基于椭圆曲线的多对一加密认证的方案设计视频会议安全机制，其优势是能够减轻服务器存储和管理密钥的负担，大大节省了服务器的存储空间。该方案不仅保证了通信数据的机密性和完整性，而且能够保证参加会议人员身份的真实性。随着加密解密算法的不断改进，其必将有更广阔的应用前景。

参 考 文 献

[1] Al-Riyami S S, Paterson K G. CBE from CL-PKE: A generic construction and efficient schemes [C]// LNCS 3386: PKC 2005. Berlin: Springer, 2005: 398-415

[2] 唐楚华. 视频会议系统的研究与实现[D]. 武汉：武汉理工大学，2011

[3] 邓秀峰，赵明生. 一种基于 SIP 的视频会议安全机制[J]. 计算机工程，2004，30(8)：106-108

[4] 李星，郭穗鸣，等. 可扩展分布式标清视频会议系统：结构和转发模型[J]. 清华大学学报，2012，52(9)：1275-1280

[5] 林喜军，孙琳，武传坤. 基于双线性映射的多对一加密认证方案[J]. 计算机研究与发展，2009(02)

[6] 邹永辉，严亚俊，等. 椭圆曲线密码体制的实现及发展现状简介[J]. 计算机时代，2005(1)

[7] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全(第二版)[M]. 北京：清华大学出版社，1998

[8] 徐彦彦，徐正权，等. 视频会议系统安全体系设计[J]. 计算机工程与应用，2006，14：208-211

[9] Phong L T, Matsuoka H, Ogata W. Stateful Identity-Based Encryption Scheme: Faster Encryption and Decryption [C]// ASIACCS' 08. Tokyo, Japan, March 2008

[10] Yao Hua-zhen, Jing Ya-tao. The Design of Video-Conference Encryption System based on H. 264. 978-1-4244-7874-3/10© 2010 IEEE

[11] Lin Xi-jun, Wu Kun-chuan, Liu Feng. Many-to-one encryption and authentication scheme and its application [J]. Journal of Communications and Networks, 2008, 10(1)

[12] Shamir A. Identity-based cryptosystems and signature schemes [C]// LNCS 196: CRYPTO 1984. Berlin: Springer, 1985: 48-53

[13] Purdy G B. A High Security Log-in Procedure[J]. Communications of the ACM, 1974, 17(8): 442-445

(上接第 174 页)

[10] Shim W, Kim G, Kim S. A distributed sinkhole detection method using cluster analysis[J]. Expert Systems with Applications, 2010, 37(12): 8486-8491

[11] Cheng B C, Tseng R Y. A context adaptive intrusion detection system for MANET[J]. Computer Communications, 2011, 34(3): 310-318

[12] 周永浩，李鸥，刘洋. 基于 SVM 的 MANET 路由层入侵检测[J]. 计算机应用研究，2010，27(5)

[13] 叶进，李伶强. 基于保护流的 MANET 网 MAC 层 DoS 攻击及防御[J]. 计算机科学，2011，38(4)：118-121

[14] 邓立博. MANET 入侵检测系统研究与实现[D]. 哈尔滨：哈尔滨工程大学，2012

[15] Mitrokotsa A, Dimitrakakis C. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection[Z]. Ad-hoc Networks, 2012