基于无证书的可验证加密签名方案

周 敏[1] 杨 波[1] 傅 贵[2,3] 巫莉莉[4]

(华南农业大学信息学院 广州 510642)[1] (华南理工大学计算机科学与工程学院 广州 510640)[2]

(广州市交通管理科学研究所 广州 510640)[3] (华南农业大学现代教育技术中心 广州 510642)[4]

摘 要 无证书密码体制实现无公钥证书且没有密钥托管的性质。将无证书加密方案与可验证加密方案相结合,提出了一种基于无证书的可验证加密签名方案(Certificateless Verifiably Encryption Signature scheme 简称 CVES),并给予该方案的正确性和不可伪造证明,该方案能有效地克服恶意签名和合谋攻击。

关键词 双线性对,无证书加密,可验证加密签名,不可伪造

中图法分类号 TP309 **文献标识码** A

Verifiably Encrypted Signature Scheme Based on Certificateless

ZHOU Min[1] YANG Bo[1] FU Gui[2,3] WU Li-li[4]

(College of Informatics, South China Agriculture University, Guangzhou 510642, China)[1]

(School of Computer Science & Engineering, South China University of Technology, Guangzhou 510640, China)[2]

(The Institute of Traffic Management, Guangzhou 510640, China)[3]

(Modern Education Technology Center, South China Agriculture University, Guangzhou 510642, China)[4]

Abstract Certificateless cryptosystem realizes the properties of the certificateless, and the key-unescrow. So Certificateless Verifiably Encrypted Signature Scheme (CVES) was proposed, which is composed of Certificateless Encryption Scheme and Verifiably Encrypted Signature Scheme. Finally, the correctness and unforgeability of CVES was proved. This scheme can effectively overcome the malicious signature and collusion attack.

Keywords Bilinear pairing, Certificateless cryptosystem, Verifiably encrypted signature, Unforgeability

1 引言

1978年 Rivest, Shamir 和 Adleman[1]第一次提出公钥加密方案。1984年 Shamir[2]引进了基于身份的密码学 IDPKC 的概念。IDPKC 消除了对用户证书的依赖,极大地简化了密钥管理问题。在 IDPKC 的研究中,一个突破性的工作是 Boneh 和 Franklin[3]提出了第一个有效的基于身份的加密方案,其构造利用了椭圆曲线上的双线性映射。

2003年 Al-Riyami 和 Paterson 提出了基于无证书的公钥加密方案(CL-PKE)[4],系统参数由系统初始化,用户的部分私钥由一个可信第三方(KGC)生成,用户使用这个部分私钥和自己生成的秘密值独立地生成自己的公钥和私钥。克服了传统公钥密码学中的证书存在问题,而且消除了基于身份密码学中密钥托管的问题。

一个可验证的加密签名方案涉及到3个参与方:签名者、验证者以及一个可信的第三方(或称仲裁者)。这类协议的基本思想是签名者根据其对某一消息的原始签名,利用仲裁者的公钥进行加密产生可验证的加密签名 ves 并发送给验证者。一个可验证的加密签名应该满足可验证性和可恢复性。可验证性是指任何验证者能够检验 ves 的确是签名者对该消息的原始签名进行的加密,但是验证者不能从中提取出原始签名;而可恢复性则意味着 ves 能够向验证者保证指定的仲裁者能够从中提取出原始的签名。

第一个非交互的可验证加密签名方案由 Boneh 等人在文献[5]中提出,该方案在随机预言模型下是可证明安全的,而且也是第一个无需在用户与 TTP 之间进行特殊注册,无需零知识证明的方案。利用 Hess 的基于身份的签名方案[6],Gu 和 Zhu 提出了一个基于身份的可验证加密签名方案[7],其突出的特点是:不仅签名者的公钥是基于身份的,而且仲裁者的公钥也是基于身份的。然而,Gu 和 Zhu 提出的可验证加密签名方案实际上是不安全的。文献[8]分析表明,对于任何消息,恶意签名者都很容易产生一个可验证的加密签名,并向任何验证者证明其有效性,但是指定的仲裁者却不能把它转化成该签名者的原始签名;此外,该协议还容易受到合谋攻击,即恶意验证者在接收到一个签名者的可验证加密签名之后,与他人合谋可以得到该签名者的原始签名。

本文用无证书加密方案与可验证加密方案相结合,提出一种新的基于无证书的可验证的加密签名方案(CVES),它

到稿日期:2009-01-16 返修日期:2009-03-06 本文受国家自然科学基金(项目编号:60773175,60673077),广州市信息安全技术(密码学)实验室课题"无证书公钥密码系统的研究"资助。

周 敏(1973-),女,博士研究生,讲师,主要研究方向为信息安全和安全多方计算,E-mail:zmfw@scau.edu.cn。

能有效地克服恶意签名和合谋攻击。

2 相关知识

2.1 双线性对

设$(G_1,+)$和$(G_2,*)$是两个阶为q的循环群，P是G_1的生成元，$e:G_1\times G_1\to G_2$是一个双线性映射，满足如下条件：

(1)双线性。对任意的$P,Q,R\in G_1$成立$e(P+Q,R)=e(P,R)e(Q,R)$和$e(P,Q+R)=e(P,Q)e(P,R)$。特别地，对任何$a,b\in Z_q^*$有$e(aP,bQ)=e(P,Q)^{ab}=e(abP,Q)=e(P,abQ)$。

(2)非退化性。存在$P,Q\in G_1$，使得$e(P,Q)\neq 1$。

(3)可计算性。存在有效的算法计算$e(P,Q)$对任意的$P,Q\in G_1$。

满足上述性质的运算e称为双线性对。

2.2 CBDH 和 DBDH 问题

(1) CBDH(Computational Bilinear Diffie-Hellman)问题：对于任意的$a,b,c\in Z_q^*$，给定$\langle P,aP,bP,cP\rangle$计算$e(P,P)^{abc}$。

(2) DBDH(Decisional Bilinear Diffie-Hellman)问题：对于任意的$a,b,c\in Z_q^*$，给定$\langle P,aP,bP,cP\rangle$和$h\in G_2$，判定$h=e(P,P)^{abc}$是否相等。

2.3 无证书加密模型

无证书加密方案的合法参与者包含：私钥生成中心KGC，签名者S，验证者R。此签名模型由如下7个多项式时间算法组成：

(1)系统参数建立：由KGC完成的概率性多项式时间算法。输入参数k，输出主密钥s。计算$P_{pub}=sP$并输出系统参数$params$。

(2)部分私钥提取：由KGC完成的确定性多项式时间算法。输入$params$、主密钥s和用户的身份$ID_i\in\{0,1\}^*$。输出用户的部分私钥D_i。

(3)设置秘密值：由用户完成的概率性多项式时间算法。输入$params$和用户的身份ID_i，输出用户的秘密值x_i。

(4)秘密钥提取：一个由用户完成的概率多项式时间算法，输入$params$、用户的部分私钥D_i和用户的秘密值x_i，输出用户的秘密钥S_i。

(5)公开钥提取：由用户完成的确定性多项式时间算法。输入$params$、用户的身份ID_i以及用户的秘密值x_i，输出用户的公钥PK_i。

(6)加密：由发送者S完成的概率性多项式时间算法。输入$params$、消息m、接收者的PK_R，输出密文C。

(7)解密：由接收者完成的确定性多项式时间算法，输入$params$、接收者的私钥S_R，输出明文m。

2.4 Gu 和 Zhu 的基于身份的可验证加密签名方案

Gu 和 Zhu 的基于身份的可验证的加密签名方案[7]由以下7个多项式时间的算法组成：

(1)Setup：给定(G_1,G_2,q,e,P)随机选取$s\in Z_q^*$并置$P_{pub}=sP$。选择密码杂凑函数$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\times G_2\to Z_{q_1}$以及$H_3:G_2\to Z_q$。系统公开参数是$params=(G_1,G_2,q,e,P,P_{pub},H_1,H_2,H_3)$。系统主密钥(即PKC的私钥)是$s$。

(2)Extract：给定用户的身份标识ID_X，PKG计算

$Q_X=H_1(ID_X)\in G_1$和$D_X=sQ_X\in G_1$

并通过安全信道把D_X传递给该用户。该用户的私钥是D_X。同样，身份标识为ID_A的仲裁者的私钥是$D_A=sQ_A\in G_1$，其中$Q_A=H_1(ID_A)\in G_1$。

(3)Sign：给定签名者的私钥D_X和消息m，随机选择$k\in Z_q^*$，计算并输出签名(r,U)，其中$r=e(P,P)^k$，$h=H_2(m,r)$，$U=hD_X+kP$。

(4)Verify：给定身份标识为ID_X的签名者对于消息m的签名(r,U)，验证者计算$h=H_2(m,r)$和$Q_X=H_1(ID_X)$，接受该签名为有效的当且仅当

$r=e(U,P)\cdot e(Q_X,P_{pub})^{-h}$。

(5)VE-Sign：给定签名私钥D_X，消息$m\in\{0,1\}^*$以及仲裁者的身份标识ID_A，首先计算$Q_A=H_1(ID_A)$，然后执行以下步骤：

随机选取$k_1,k_2\in Z_q^*$；

计算$r=e(P,P)^{k_1}$，$h=H_2(m,r)$，$h'=H_3(e(Q_A,P_{pub})^{k_2})$；

计算$U_1=h'P$，$U_2=k_2P$，$V=hD_X+(k_1+h'k_2)P+h'Q_A$；

输出可验证加密签名(r,V,U_1,U_2)。

(6)VE-Verify：给定身份标识为ID_X的签名者对于消息m的可验证加密签名(r,V,U_1,U_2)首先计算$h=H_2(m,r)$，$Q_X=H_1(ID_X)$然后接受该签名当且仅当

$$e(P,V)=r\cdot e(hP_{pub},Q_X)\cdot e(U_1,Q_A+U_2) \quad (1)$$

(7)Adjudication：给定仲裁者的私钥$D_A=sQ_A$以及身份标识为ID_X的签名者对于消息m可验证的加密签名(r,V,U_1,U_2)首先通过式①验证其有效性，如果验证通过，则计算$U=V-H_3(e(D_A,U_2))(Q_A,+U_2)$，并输出$(r,U)$作为身份标识为$ID_X$的签名者对于消息$m$的原始签名。

实际上，由(Setup,Extract,Sign,Verify)组成的签名算法就是Hess的基于身份的签名方案[6]。

Gu 和 Zhu 在随机预言模型下证明了其方案满足两个性质：非伪造性和不透明性。然而 Gu-Zhu 的方案并不能达到一个可验证的加密签名方案所必须满足的可验证性和可恢复性。其原因在于验证者是无法检验$U_1=h'P$是否成立的。此外！注意到验证方程①并不保证同一个k_2被签名者用于计算$U_2=k_2P$和$h'=H_3(e(Q_A,P_{pub})^{k_2})$，因此签名者在不知道$h'$的情况下也可以产生有效的可验证加密签名。因此该协议存在合谋攻击[8]。

合谋攻击是Bao[9]于Asiacrypt 04上提出来的：验证者接收到签名者ID_X对消息m的可验证的加密签名ves之后，与另一个签名者B进行合谋，B根据ves产生自己合法的可验证加密签名ves'，并声称在验证者与B之间发生了争执，请求仲裁者对ves'进行仲裁，然后利用对ves'的仲裁结果从ves中计算出ID_X的原始签名。如果合谋攻击成功，那么公平交换中的一方不用出示自己对消息m的签名就可以得到对方的签名，所以这是对公平交换协议的重要危害。

3 基于无证书的可验证加密签名方案

通过对基于无证书加密和可验证加密的分析研究，提出一种基于无证书的可验证加密签名方案(CVES)。

基于无证书的可验证加密签名方案由以下10个步骤组

成：

(1)系统参数建立：给定(G_1,G_2,q,e,P)随机参数 $s\in Z_q^*$ 并置 $P_{pub}=sP$。选择 3 个 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\times G_2\rightarrow Z_{q_1}$ 以及 $H_3:G_2\rightarrow Z_q$。系统公开的参数$(G_1,G_2,q,e,P,P_{pub},H_1,H_2,H_3)$。系统的主密钥为 s。

(2)提取部分私钥：身份 $ID_i\in\{0,1\}^*$ 作为输入，KGC 计算 $Q_i=H_1(ID_i)\in G_1$，输出部分私钥 D_i，$D_i=sQ_i\in G_1$。

(3)设置秘密值：用户随机选取 $x_i\in Z_q^*$ 作为自己的秘密值。

(4)设置秘密钥：用户计算自己的私钥，$S_i=x_iD_i=x_isQ_i$。

(5)设置公开钥：用户计算自己的公钥 $PK_i=(X_i,Y_i)=(x_iP,x_iQ_i)$。

(6)签名：给定签名者的私钥 S_i 和消息 m，随机选择 $k\in Z_q$，计算并输出签名(r,U)，其中 $r=e(P,P)^k$，$h=H_2(m,r)$，$U=hS_i+kP$。

(7)验证：给定身份标识为 ID_i 的签名者对消息 m 的签名(r,U)，验证者计算 $h=H_2(m,r)$和 $Q_i=H_1(ID_i)$，接受该签名为有效的当且仅当 $r=e(U,P)\cdot e(Y_i,P_{pub})^{-h}$。

(8)CVES 加密签名：给定签名私钥 S_i，消息 $m\in\{0,1\}^*$，执行以下步骤：

随机选取 $k_1\in Z_q^*$

a) 计算 $a=x_iY_A$，$b=e(a,P_{pub})$，其中 Y_A 代表仲裁者的公开钥

b) 计算 $r=e(P,P)^{k_1}$，$h=H_2(m,r)$，$h'=H_3(e(Y_A,P_{pub})^b)$

c) 计算 $U_1=h'P$，$U_2=bP$，$V=hS_i+(k_1+h'b)P+h'Y_A$

输出无证书的可验证加密签名(r,V,U_1,U_2)。

(9)CVES 解密验证：给定身份 ID_i 的密值 x_i 的签名者对消息 m 的无证书的可验证加密签名(r,V,U_1,U_2)。

a) 计算 $b=e(S_A,X_i)$，其中 S_A 代表仲裁者的秘密钥；

b) 计算 $h=H_2(m,r)$，$Q_i=H_1(ID_i)$；

c) 当且仅当 $e(P,V)=r\cdot e(hP_{pub},Y_i)\cdot e(U_1,Y_A+U_2)$。接受该签名，否则拒绝。

(10) Adjudication：给定仲裁者的私钥 $S_A=sQ_A$ 以及身份标识为 ID_i 的签名者对消息 m 可验证的加密签名(r,V,U_1,U_2)，首先通过(9)步中 c)里的公式验证其有效性，如果验证通过，则计算 $U=V-H_3(e(S_A,U_2))(Y_A,+U_2)$，并输出$(r,U)$作为身份标识为 ID_X 的签名者对于消息 m 的原始签名。

4 基于无证书的可验证加密签名方案的分析

基于无证书的可验证加密签名方案，能有效地克服恶意的签名者与合谋攻击，下面对其性质作出相应的分析。

4.1 正确性

验证者接收签名，因为下列等式成立。

$$e(U,P)\cdot e(Y_i,P_{pub})^{-h}=e(U,P)\cdot e(x_iQ_i,sP)^{-h}$$
$$=e(U,P)\cdot e(x_isQ_i,P)^{-h}$$
$$=e(hS_i+kP,P)\cdot e(S_i,P)^{-h}=e(hS_i+kP,P)\cdot e(-hS_i,P)$$
$$=e(kP,P)=e(P,P)^k=r$$

(1)可验证

$$e(P,V)=e(P,hS_i+(k_1+h'b)P+h'Y_A)$$
$$=e(P,hS_i)\cdot e(P,k_1P)\cdot e(P,h'bP)\cdot e(P,h'Y_A)$$
$$=e(P,hx_isQ_i)\cdot e(P,k_1P)\cdot e(h'P,bP)\cdot e(h'P,Y_A)$$
$$=e(hsP,x_iQ_i)\cdot e(P,P)^{k_1}\cdot e(h'P,bP)\cdot e(h'P,Y_A)$$
$$=r\cdot e(hP_{pub},x_iQ_i)\cdot e(U_1,U_2)\cdot e(U_1,Y_A)$$
$$=r\cdot e(hP_{pub},Y_i)\cdot e(U_1,Y_A+U_2)$$

(2)可恢复

仲裁者解加密签名得到原始签名中的 U：

$$U=V-H_3(e(S_A,U_2))(Y_A+U_2)$$
$$=hS_i+(k_1+h'b)P+h'Y_A-H_3(e(S_A,U_2))(Y_A+U_2)$$
$$=hS_i+k_1P+h'bP+h'Y_A-H_3(e(x_AsQ_A,bP))(Y_A+U_2)$$
$$=hS_i+k_1P+h'(bP+Y_A)-H_3(e(bx_AQ_A,sP))(Y_A+U_2)$$
$$=hS_i+k_1P+h'(U_2+Y_A)-H_3(e(bY_A,P_{pub}))(Y_A+U_2)$$
$$=hS_i+k_1P+h'(U_2+Y_A)-H_3(e(Y_A,P_{pub})^b)(Y_A+U_2)$$
$$=hS_i+k_1P+h'(U_2+Y_A)-h'(Y_A+U_2)$$
$$=hS_i+k_1P$$

仲裁者解加密签名得到原始签名中的 r：

$$e(P,U)\cdot e(Y_i,P_{pub})^{-h}=e(P,U)\cdot e(x_iQ_i,sP)^{-h}$$
$$=e(P,U)\cdot e(-hx_isQ_i,P)$$
$$=e(P,U)\cdot e(-hS_i,P)=e(U-hS_i,P)=e(k_1P,P)=r$$

则仲裁者输出(r,U)作为身份标识为 ID_i 的签名者对于消息 m 的原始签名。

(3)仲裁者可以验证 U_1 的正确性

$$b=e(S_A,X_i)=e(x_AsQ_A,x_iP)$$
$$=e(sY_A,x_iP)=e(x_iY_A,sP)=e(a,P_{pub})$$
$$U_1=H_3(e(Y_A,P_{pub})^b)P=h'P$$

4.2 不可伪造性

定理 1 无证书可验证加密签名方案在适应性选择明文，身份和可验证加密签名攻击下是不可伪造的(existential unforgeable secure under adaptively chosen message, ID and verifiably encrypted signature attacks, EUF-ACMISA)。前提是 CBDH 和 DBDH 是困难的。

证明：因为本方案采用的加密签名过程和文献[7]中的一致，所以加密签名的不可伪造性等同于文献[7]中方案加密签名的不可伪造性。具体证明参见文献[7]。

4.3 可克服恶意签名

在 Gu-zhu 方案中，注意到 h'的值只能由原始签名者和仲裁者才能够计算出来，验证者无法检验 $U_1=h'P$ 是否成立。因此，不诚实的签名者可以产生一个虚假的可验证加密签名 *ves*，对于任何验证者来说，该 *ves* 看起来都是有效的。然而，仲裁者却并不能从中提取出一个有效的普通签名[8]。

本方案签名者计算 $h'=H_3(e(Y_A,P_{pub})^b)$，而仲裁者通过计算 $b=e(S_A,X_i)$就可以验证 h'。仲裁者对 U_1，U_2和 V 都可以验证正确性。这样避免了不诚实的签名者产生虚假的无

证书可验证加密签名 ves。克服了 Gu-Zhu 方案存在恶意签名性的弱点。

4.4 可克服合谋攻击

在 Gu-zhu 方案中，注意到验证方程① 并不保证同一个 k_2 被签名者用于计算 $h'=H_3(e(Q_A,P_{pub})^{k_2})$ 和 $U_2=k_2P$，$V=hD_X+(k_1+h'k_2)P+h'Q_A$，因此签名者在不知道 h' 的情况下也可以产生有效的可验证加密签名。这一发现导致了该协议存在合谋攻击[8]。

本方案中，取消参数 k_2，用 b 替代。$a=x_iY_A$，$b=e(a,P_{pub})$，从等式中知 b 的产生需要签名者的秘密值 x_i 和仲裁者的公开钥 Y_A。验证时 $b=e(S_A,X_i)$，计算 b 需要签名者的公开钥 X_i 和仲裁者的秘密钥 S_A。因为 $h'=H_3(e(Y_A,P_{pub})^b)$ 是可验证的，所以 $U_1=h'P$ 也可以验证，因而就避免了合谋攻击者通过利用 U_1 计算自己的可验证加密签名而进行计算原始签名的可能。

结束语 本文研究分析了无证书签密方案和 Gu-Zhu 的基于身份的可验证加密签名方案后，结合无证书和可验证签名，提出了基于无证书的可验证的加密签名方案，证明了该方案的正确性和不可伪造性，以及它可以有效避免 Gu 和 Zhu 提出的可验证加密签名方案存在的恶意签名和合谋攻击。

参 考 文 献

[1] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21: 120-126

[2] Shamir A. Identity based cryptosystems and signature schemes [C]// Proceedings of the Advances in Cryptology-Cryipto'84. Lecture Note in Computer Science: 196. Springer-Verlag, 1984: 47-53

[3] Boneh D, Franklin M. Identity - base encryption from the Well pairing[C]// Proceedings of the Advances in Cryptology-Crypto 2001. Lecture Note in Computer Science: 2139. Springer-Verlag, 2001: 213-229

[4] Al-Riyami S S, Paterson K. Certificateless Public Key Cryptography[C]// Proc. of Asiacrypt'03. [S. l.]: Springer-Verlag, 2003

[5] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]// Proceedings of the EUROCRYPT' 03. LNCS, vol. 2656. Berlin: Springer, 2003: 416-432

[6] Hess F. Efficient identity based signature schemes based on pairings[C]// Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography. Lecture notes in Computer Science ; 2595. Springer-Verlag, 2003: 310-324

[7] Gu C X, Zhu Y F. An ID-based verifiable encrypted signature scheme based on Hess's scheme[C]// Proceedings of the 1st SKLOIS Conference on Information Security and Cryptology. Lecture Notes in Computer Science: 3822. Springer-Verlag, 2005: 42-52

[8] 张振峰. 基于身份的可验证加密签名协议的安全性分析[J]. 计算机学报, 2006, 29(9): 1688-1693

[9] Bao F. Colluding attacks to a payment protocol and two signature exchange schemes[C]// Proceedings of the Advances in Cryptology-ASIACRYPT 2004. Lecture Notes in Computer Science: 3329. Spring-Verlag, 2004: 417-429

(上接第 85 页)

[2] Akyildiz I F, Wang X, Wang W. Wireless mesh networks: a survey[J]. Computer Networks, 2005, 47(4): 445-487

[3] Medina A, Allman M, Floyd S. Measuring the evolution of transport protocols in the internet[J]. ACM SIGCOMM Computer Communication Review, 2005, 35(2): 37-51

[4] Holland G, Vaidya N. Analysis of TCP Performance over Mobile Ad Hoc Networks[J]. Wireless Networks, 2002, 8(2/3): 275-288

[5] Lohier S, Doudane Y G, Pujolle G. Cross-Layer Loss Differentiation Algorithms to Improve TCP Performance in WLANs[C]// Proceedings of the 11th IFIP TC6 International Conference on Personal Wireless Communications (PWC'06). vol. 4217 of LNCS. Springer, 2006: 297-309

[6] Barman D, Matta I. Effectiveness of Loss Labeling in Improving TCP Performance in Wired/Wireless Networks[C]// Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02). IEEE Press, 2002: 2-11

[7] Biaz S, Vaidya N H. Discriminating Congestion Losses from Wireless Losses Using Inter-Arrival Times at the Receiver[C]// Proceedings of the 2nd IEEE Symposium on Application-Specific Systems and Software Engineering Technology (ASSET'99). IEEE Press, 1999: 10-17

[8] Cen S, Cosman P C, Voelker G M. End-to-End Differentiation of Congestion and Wireless Losses[J]. IEEE/ACM Transactions on Networking, 2003, 11(5): 703-717

[9] Chandran K, et al. A Feedback - Based Scheme for Improving TCP Performance in Ad Hoc Wireless Networks[J]. IEEE Personal Communications, 2001, 8(1): 34-39

[10] Eddy W M, Ostermann S, Allman M. New techniques for making transport protocols robust to corruption-based loss[J]. SIGCOMM Computer Communication Review, 2004, 34(5): 75-88

[11] 刘俊, 隆克平, 徐昌彪, 等. 两种改善无线 TCP 性能的新机制[J]. 电子学报, 2004, 32(12): 2059-2062

[12] Khayat I E, Geurts P, Leduc G. Enhancement of TCP over Wired/Wireless Networks with Packet Loss Classifiers Inferred by Supervised Learning[R]. Research Unit in Networking, University of Liège, 2004

[13] Bhandarkar S, Sadry N E, Reddy A L N, et al. TCP-DCR: A Novel Protocol for Tolerating Wireless Channel Errors[J]. IEEE Transactions on Mobile Computing, 2005, 4(5): 517-529

[14] Paul R, Trajkovic L. Selective - TCP for Wired / Wireless Networks[C]// Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06). 2006

[15] NS-2 Network Simulator (Ver. 2) LBL[OL]. http://www.mash.cs.berkly.edu/ns/

[16] Johnson D B, Maltz D A, Hu Y C, et al. The dynamic source routing protocol for mobile ad hoc networks[M]. IETF Draft MANET Working Group, 2000

[17] Padhye J, Firoiu V, Towsley D, et al. Modeling TCP throughput: A simple model and its empirical validation[C]// Proceedings of SIGCOMM'98. 1998

[18] Liu J, Singh S. ATCP: TCP for Mobile Ad-Hoc Networks[J]. IEEE Journal on Selected Areas in Communications, 2001, 19(7): 1300-1315