基于身份的分布式卫星网络私钥管理方案

吴 杨 矫文成 潘艳辉 李 华
(军械工程学院计算机工程系 石家庄 050003)

摘 要 针对卫星网络节点私钥分量更新过程的消息篡改攻击威胁,提出了双重数据加密方案,以保障私钥分量更新过程中数据的完整性。为防止拥有合法身份恶意节点发起的强制私钥分量更新申请,建立了节点私钥分量更新申请时刻合法性判断机制,以抵制拥有合法身份的恶意节点发起的拒绝服务攻击。最后,对比分析了方案的安全性和计算复杂度,结果表明,通过引入较低的额外计算开销实现了有效抵御节点私钥分量更新过程的消息篡改攻击和拒绝服务攻击。

关键词 分布式卫星网络,消息篡改攻击,私钥,拒绝服务攻击
中图法分类号 TP309 **文献标识码** A

Id-based Private-key Management Scheme in Distributed Satellite Network

WU Yang JIAO Wen-cheng PAN Yan-hui LI Hua
(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract In order to prevent data modification attack in process of private-key component update of satellite network node, we presented a double-encryption scheme, which can ensure integrity of data in process of private-key component update. At the same time, to prevent violent private-key component updating request from venomous node with normal identity, a mechanism was provided to judge the validity of update request time, which can resist denial of service attack from venomous node with normal identity. Finally, we compared the security and computing complexity of the scheme, it shows that by introducing low computing costs, the scheme we provided can resist data modification attack and denial of service attack.

Keywords Distributed satellite network, Data modification attack, Private-key, Denial of service attack

1 引言

Shamir于1984年在美国密码学会议上提出的基于身份的公钥密码系统[1],大大降低了公钥系统的复杂度。2001年,Boneh和Franklin采用双线性对技术[2],提出了第一个真正意义上基于身份的加密机制(IBE)。为解决密钥管理的单点失效问题,Zhou与Hass等人提出了基于分布式CA(Certificate Authority)的密钥管理模型[3],并将其运用到了Ad-hoc网络中。

文献[4]使用双线性对技术和门限共享机制,实现了基于身份的Ad-hoc网络的密钥管理方案,但其方案并不能抵御内部恶意节点的频繁私钥分量更新申请,且在私钥分量更新过程中缺乏双向认证机制。文献[5]结合Ad-hoc网络与卫星网络的相似性,将基于分布式CA的密钥管理方案引入空间网络密钥管理,但协议仍需要依靠证书实现认证。为克服卫星网络密钥管理过程中证书维护难题,文献[6]提出了基于身份的空间网络会话密钥协商方案,但未考虑节点私钥更新问题。在此基础上,文献[7]提出了分布式网络中基于IDPKC的私钥更新方案,文献[8]在上述文献基础上提出了基于身份的空间网络私钥管理方案,实现了密钥管理过程中空间节点间身份的双向认证,并提出了避免出现空间节点私钥分量更新请求拥塞的方案。研究表明,文献[8]提出的方案不能有效抵御消息篡改攻击行为;普通节点发起私钥分量更新请求时,应答节点未对其申请时刻的合法性进行判断,该方案也无法抵制拥有合法身份的恶意节点发起的拒绝服务攻击。

在此基础上,本文提出了一种改进的基于身份的分布式卫星网络私钥管理方案,其能够有效地抵御卫星节点私钥更新过程中的消息篡改攻击。应答节点在接受私钥分量更新申请时,将对申请时刻的合法性进行判断,抵御恶意节点发起的拒绝服务攻击。

本文第2节介绍了方案相关原理;第3节阐述了方案的实现过程;第4节对比分析了本文与文献[8]方案的安全性及运算复杂度;最后对本文工作进行了总结。

2 相关知识

利用椭圆曲线上的Weil对和Tate对构造基于双线性对的密码系统,是目前一致采用的有效途径。下面介绍双线性映射对及其性质。

到稿日期:2010-11-15 返修日期:2011-02-25 本文受国家自然科学基金项目(60772082)资助。

吴 杨(1985-),男,硕士生,主要研究方向为网络安全与密码学,E-mail:baiyanwy@163.com;矫文成(1970-),男,副教授,硕士生导师,主要研究方向为信息安全与软件工程;潘艳辉(1982-),女,博士,主要研究方向为网络安全;李 华(1981-),男,博士,主要研究方向为网络安全。

设 G_1 和 G_2 分别为循环加法群和乘法群，其阶数为素数 q。定义 $e:G_1\times G_1\to G_2$ 为一个双线性映射，且满足：

(a)双线性：对任意 $a,b\in Z_p$，$P,Q\in G_1$，有 $e(aP,bQ)=e(P,Q)^{ab}$ 成立；

(b)非退化性：存在 $P\in G_1$，满足 $e(P,P)\neq 1$；

(c)可计算性：若 $P,Q\in G_1$，则可以在多项式时间内有效计算出 $e(P,Q)$。

本文提出的分布式卫星网络私钥更新方案，依赖以下难题：

定义 1 若 G_1,G_2 是阶同为素数 q 的循环群，且有双线性映射 $e:G_1\times G_1\to G_2$，P 为 G_1 的生成元，则在 $\langle G_1,G_2,e\rangle$ 上的 Bilinear Difie—Hellman(BDH)问题是：给定 $a,b,c\in Z_P$：由 $\langle P,aP,bP,cP\rangle$ 计算 $e(P,P)^{abc}$。

定义 2 设 G_1,G_2 是阶为素数 q 的循环群，且有双线性映射 $e:G_1\times G_1\to G_2$，G_1 的生成元为 P，则 $\langle G_1,G_2,e\rangle$ 上的 Decisional Bilinear Difie—Hellman(DBDH)问题可描述为：由任意 $a,b,c\in Z_P$，由 $\langle P,aP,bP,cP\rangle$ 和 $h\in G_2$ 判断 $h=e(P,P)^{abc}$ 是否成立。

3 方案研究与实现过程

3.1 卫星通信面临的主要安全威胁

卫星网络采用广播通信方式进行信息传递。在卫星节点计算及存储等资源受限的情况下，卫星通信更易受到主动攻击及被动攻击威胁。主动攻击的主要形式有：重放攻击、信息篡改攻击、拒绝服务攻击等。重放攻击：主要通过发送目标节点已接收过的数据包，来达到欺骗目标节点的目的。信息篡改攻击：针对信息完整性而发起的对信息进行恶意修改而不被察觉的攻击。拒绝服务攻击：主要是对目标系统的计算资源及网络带宽资源进行恶意消耗，以达到降低系统效率或致系统瘫痪的目的。被动攻击主要是以搭线窃听的方式，收集目标系统的相关信息，且不易被察觉。卫星网络的广播通信方式更使其面临严重的被动攻击威胁。

3.2 卫星网络密钥协商特点及需求

结合现有密钥管理技术与卫星网络特点，卫星网络密钥管理的主要特点及需求为：(1)卫星网络卫星节点信息存储空间及计算能力有限，对卫星网络密钥协商协议的计算复杂度提出了很高的要求，因此，卫星网络密钥协商协议应使用较小的存储空间并具有较低的计算复杂度；(2)有限的卫星网络带宽给卫星网络密钥协商过程中的节点信息交互次数提出了新的要求，因此卫星网络密钥协商协议应具有较少的交互次数，以降低通信开销；(3)面对复杂的空间环境及传输信息的机密性，卫星网络密钥协商协议必须具有较高的安全性，以确保密钥及信息的安全性；(4)动态变化的卫星网络结构大大增加了密钥协商的难度，因此，卫星网络密钥协商协议应适应不断变化的卫星网络结构。

3.3 分布式卫星网络密钥管理模型

分布式卫星网络私钥管理方案的网络模型如图 1 所示。PKG 为地面掌握完整主密钥的私钥生成中心，DPKG 节点为分布在卫星网络空间、拥有主密钥份额的分布式私钥分量产生节点。PKG 负责卫星网络空间节点的初始私钥产生和分发，DPKG 节点主密钥份额的更新也由 PKG 完成。为提高系统安全性，本文假定 PKG 选择的 DPKG 节点比普通空间节点更具抗攻击能力，即 DPKG 节点比普通空间节点具有更高的安全性，例如 PKG 可以选择具有入侵检测系统或其他一些安全防护设备的空间节点作为 DPKG 节点。PKG 选择空间 DPKG 节点时，应尽量使 DPKG 节点在网络中分布均匀。为便于管理卫星网络节点，任一卫星节点被赋予唯一 ID 标志(MAC 或 IP 地址)。

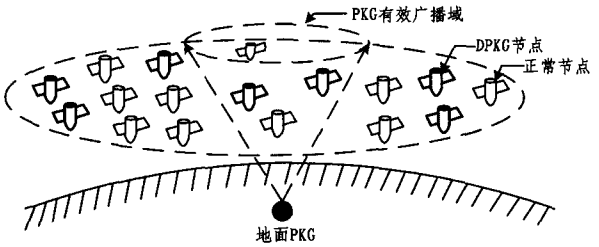

图 1 分布式卫星网络模型

3.4 方案实现过程

3.4.1 系统初始化

系统初始化阶段，PKG 选择参数如下：

(1)选择阶为 q、生成元为 P 的循环加法群 G_1、循环乘法群 G_2。(2)双线型映射 $e:G_1\times G_1\to G_2$。(3)定义安全 Hash 函数：$H_1:\{0,1\}^*\to G_1$ 将字节串映射为 G_1 上的点，$H_2:G_2\to\{0,1\}^*$ 将循环乘法群 G_2 上的点映射为字节串。(4)PKG 随机选取 $s\in Z_P^*$ 作为系统主密钥，计算 $P_{pub}=sP\in G_1$。(5)系统初始化时 PKG 令 $m=m_0(m_0\neq 0)$，PKG 为任意卫星节点 A 计算其初始公私钥对 $\langle K_A,K_A^{-1}\rangle$，其中 $K_A=H_1(ID_A\|m_A)$，$K_A^{-1}=sK_A$。(6)产生主密钥共享多项式(其中 $a_i\in Z_P$)：$f(x)=(s+\sum_{i=0}^{t-1}a_ix^i)\bmod q$，且 $f(0)=s$。(7)PKG 选择 n 个符合要求的 DPKG 节点，对任意 DPKG 节点 v，PKG 计算其初始主密钥份额 $s_V=f(ID_V)$，资格验证参数 $S_V=s_VsP$。(8)设置普通卫星节点私钥更新周期为 w。(9)构造映射 $g:ID\to T$，在系统密钥更新周期内，实现所有普通卫星节点私钥分量更新时刻的均匀分布，并根据节点 ID 为其生成私钥分量更新时刻集合。由所有普通卫星节点 ID 和映射函数 g，最终可形成普通卫星节点私钥分量更新时刻图。(10)根据实际网络特点，设置网络最大传输时延 Δt。PKG 完成对系统的初始化后，公开如下参数：

$$\{P,q,P_{pub},G_1,G_2,e,H_1,H_2,m_0,w,g,\Delta t\}$$

3.4.2 新节点加入

若有新节点 A 加入网络，PKG 根据其 ID 计算其初始公私钥对 $\langle K_A,K_A^{-1}\rangle$。所有 DPKG 节点将根据节点私钥分量更新时刻图，结合当前系统时刻，检测申请节点申请更新私钥分量时刻的合法性。由节点 ID 和映射函数 g 得到节点在系统密钥更新周期内的私钥分量更新时刻图。如图 2 所示，gp_i 为在 t_i 时刻申请私钥分量更新的卫星节点集合。

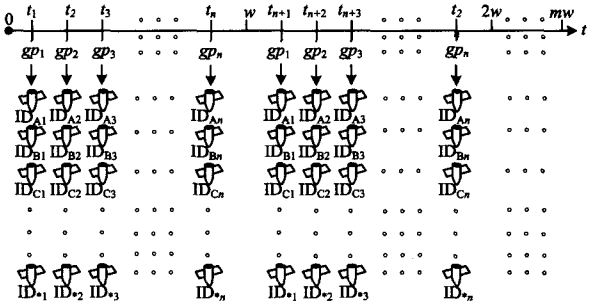

图 2 卫星节点私钥分量更新时刻图

3.4.3 节点私钥更新

PKG完成系统的初始化后，在系统∂时刻节点A公私钥对$\langle K_A, K_A^{-1}\rangle$到期，节点$A$更新获得其新公私钥对$\langle K_{A_NEW}, K_{A_NEW}^{-1}\rangle$过程如下。

节点A通过如下方法计算其新公钥K_{A_NEW}：

(1)计算首次私钥更新时间：$\partial_A = g(ID_A)$；

(2)计算私钥更新次数：$m_A = (\partial - \partial_A)/w$；

(3)计算新公钥值：$K_{A\_NEW} = H_1(ID_A || m_0 + m_A + 1)$。

节点A申请新$K_{A_NEW}^{-1}$过程如下。

(1)节点A任选$r_A \in Z_{P^*}$，计算$R_A = r_A P$，$Sig_A = r_A K_A + K_A^{-1}$，节点$A$向至少$l$个DPKG节点广播如下信息($l$为共享多项式门限值)：

$REQ_{update} = \{R_A, K_{A\_NEW}, Sig_A, ID_A\}$

(2)收到私钥更新请求的DPKG节点X首先记录当前系统时刻t，并验证$e(Sig_A, P) = e(K_A, R_A + P_{pub})$是否成立。若等式不成立，则拒绝节点$A$私钥更新请求；若成立，进一步判断节点$A$申请时刻的合法性。

(3)节点X根据节点A的ID_A和映射函数g，获得节点A私钥分量合法更新时刻集合T_A，判断是否存在元素$t_i \in T_A$使得$|t_i - t| \leqslant \Delta t$成立。若不等式不成立，则拒绝节点$A$私钥分量更新请求；若成立，则继续私钥更新过程。

(4)节点X根据其当前主密钥分量s_X，为节点A计算新私钥分量：$M_X = s_X K_{A\_NEW}$，并随机选择$r_X \in Z_{P^*}$，令$U = M_X + r_X R_A$，$R_X = r_X P$，$H_X = s_X P_{pub}$，计算$E(\{U, R_X, H_X, S_X\}, K_A)$后，向节点$A$发送$E(\{U, R_X, H_X, S_X\}, K_A)$。

(5)申请节点A收到节点X应答信息后，用私钥K_A^{-1}解密，获得$\{U, R_X, H_X, S_X\}$。验证$e(H_X, K_{PKG}) = e(P, S_X)$是否成立。若不成立，则丢弃应答消息；若成立，则计算获得X签发的私钥分量$M_X = s_X K_{A_NEW} = U - r_X R_A = U - r_A r_X P = U - r_A R_X$。

(6)节点A计算获得M_X后，验证$e(M_X, P_{pub}) = e(K_{A_NEW}, H_X)$是否成立。若等式不成立，则丢弃$M_X$；若成立，则接受$M_X$。

(7)节点A收到l个验证合格的私钥分量后(Λ为l个DPKG应答节点集合)，重构新私钥：

$K_{A\_NEW}^{-1} = \sum x \in \Lambda \lambda_x(0) M_x = \sum x \in \Lambda \lambda_x(0) s_x K_{A\_NEW} = sK_{A\_NEW}$

通过以上步骤，节点A获得了新的公私钥对$(K_{A_NEW}, K_{A_NEW}^{-1})$。

3.4.4 节点会话密钥生成

下面将介绍节点A与B间会话密钥K_S的建立过程：

(1)节点A任意选择$a \in Z_{P^*}$；

(2)计算$R_A = aP$，发送R_A给节点B；

(3)节点B任意选择$b \in Z_{P^*}$；

(4)计算$R_B = bP$，发送R_B给节点A；

(5)节点A收到R_B后计算：

$K_{AB} = H_2(e(aK_B, P_{pub})) \oplus H_2(e(K_A^{-1}, R_B))$；

(6)节点B收到R_A后计算：

$K_{BA} = H_2(e(bK_A, P_{pub})) \oplus H_2(e(K_B^{-1}, R_A))$。

由双线性对性质可知：$K_S = K_{AB} = K_{BA}$。由此，节点A、B一次交互可确定会话密钥K_S。

4 方案安全性及计算复杂度分析

4.1 安全性分析

(1)私钥分量信息传输安全性

文献[8]方案：节点A通过DPKG节点X验证后，节点X为其生成新的私钥分量M_X，利用椭圆曲线离散对数问题，DPKG节点X将M_X加密发送给申请节点A。然而，若攻击者B截获DPKG节点X发送给申请节点A的应答消息RES_{update}，B可随机选择$a \in Z_{P^*}$，将节点X的应答消息改为$aRES_{update}$，并将其重新发送给申请者A。此时，消息$aRES_{update}$依然能够通过A的验证。A最终由$aRES_{update}$计算得到aM_X作为其新的私钥分量。采用如上方式，攻击者B可破坏DPKG节点X和申请节点A间信息的完整性，而申请节点A不能有效检测和防御此类消息篡改攻击。

本文方案：节点A通过DPKG节点X验证后，节点X为其生成新的私钥分量M_X，利用椭圆曲线离散对数问题，节点X将M_X加密。为抵抗信息传递过程中消息篡改攻击，节点X使用A的公钥K_A，再对信息进行加密并将其发送给A，实现对应答消息的双重加密。应答消息传递过程中，不具有节点A私钥的节点不能解密消息，攻击者从而无法实现消息篡改攻击。

(2)私钥分量更新申请安全性分析

文献[8]方案：DPKG节点不具有对私钥分量更新申请节点申请时刻合法性的判断能力。若卫星网络中存在拥有合法身份的恶意节点，其可在任意时刻向DPKG节点提出更新私钥分量申请。由于DPKG节点未对申请节点的申请时刻合法性进行检测，DPKG节点将接受其任意时刻更新请求，并为其产生新的私钥分量。因此，恶意节点的频繁私钥分量更新申请可消耗DPKG节点的计算及通信资源，并对DPKG节点发起拒绝服务攻击。

本文方案：DPKG节点收到节点私钥分量更新申请后，记录收到更新请求的系统时刻t，并根据映射函数g和申请节点ID获得申请节点在系统密钥更新周期内的合法申请时刻集合T。DPKG节点根据申请节点私钥分量申请时刻合法性判断规则，判断申请节点申请时刻合法性。本文提出的节点私钥分量更新申请时刻合法性判断规则，能够检测和抵御拥有合法身份的恶意节点对DPKG节点发起的拒绝服务攻击。

4.2 计算复杂度分析

表1 方案计算复杂度对比

	操作类型	申请节点开销	应答节点开销
文献[8]方案	私钥更新	1MG+(2+h)MD+4he+(1+h)PA+1I	(Nh/n)(4MD+2e+2PA)
	会话密钥生成	1MG+2MD+2e	1MG+2MD+2e
本文方案	私钥更新	1MG+(2+h)MD+4he+(1+h)PA+1I+hDS	(Nh/n)(4MD+2e+2PA)+1EP+1CL
	会话密钥生成	1MG+2MD+2e	1MG+2MD+2e

下面将从系统建立计算开销、私钥更新计算开销、会话密钥生成开销角度出发，对比分析方案计算复杂度。所涉及主要运算有：双线性对运算e；字节串到G_1上点映射运算MG；G_1上数乘运算MD；G_1上点加运算PA；插值运算I；使用公钥加密运算EP，使用私钥解密运算DS；申请时刻合法性检测运算CL。节点恢复共享多项式的门限值设为h，DPKG节点

数为 n，普通节点数为 N。本文所提方案与文献[8]方案的对比结果如表 1 所列。

如表 1 所列，本文提出的方案可增强系统抵御消息篡改攻击能力，在申请节点私钥更新阶段，与文献[8]方案相比，申请节点使用其私钥额外进行 h 次解密运算。为抵御消息篡改攻击和拥有合法身份的恶意节点发起的拒绝服务攻击，DP-KG 节点增加的运算量为 1EP+1CL。

由以上分析可知，本文方案在满足文献[7,8]方案所具有的安全特性基础上，申请节点仅增加 hDS 的计算开销、应答节点增加 1EP 的计算开销，即可使系统具有抗消息篡改攻击能力；应答节点仅增加 1CL 计算开销，即能够抵御拥有合法身份恶意节点发起的拒绝服务攻击。

结束语 构建合理的卫星网络密钥管理方案，关键在于怎样平衡效率与安全需求。提出的改进方案具有如下特点：在增加较小计算开销基础上，能够抵御消息篡改攻击行为，能有效检测拥有合法身份的恶意节点发起的频繁更新私钥分量申请，抵御恶意节点发起的拒绝服务攻击。提出的方案为设计与构建卫星网络安全密钥管理方案提供了一定的思路。

参 考 文 献

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]// Proc. of CRYPTO'84. New York, USA: [s. n]. 1984: 47-53

[2] Boneh D, Franklin M. Dentity-based encryption from the Weil pairing [C]// Advances in Cryptology CRYPTO 2001. Berlin: Springer-Verlag, 2001: 213-229

[3] Zhou L, Hass Z J. Securing Ad-hoc networks [J]. IEEE Networks, 1999, 13(6): 24-30

[4] 吴平，王保云，徐开勇. 基于身份的 Ad-hoc 网络密钥管理方案[J]. 计算机工程，2008，34(24)：143-145

[5] 杨德明，慕德俊，许钟. Ad hoc 空间网络密钥管理与认证方案[J]. 通信学报，2006，27(8)：104-107

[6] 彭长艳，沈亚敏，王剑，等. 基于身份的空间网络安全研究[J]. 飞行器测控学报，2008，27(3)：56-62

[7] 李伟，罗长远，初晓. 分布式网络中基于 IDPKC 的私钥更新方案[J]. 计算机应用，2009，29(7)：1825-1827

[8] 李伟. 空间信息网络密钥管理研究[D]. 郑州：解放军信息工程大学，2009

(上接第 74 页)

因为网络延迟而造成对未失效节点的误判；(2)在检测节点与被检测节点同处一个局域网内时，即在组 1 内，算法 1 和算法 2 对未失效的误判次数要低于在组 2 内的。(3)在网络延迟时间很短的情况下，算法 1 和算法 2 在误判次数上并无太大差异，但在网络延迟时间较长的情况下，由于算法 2 增加了信任度变量和修正比例因子，因此算法 2 的误判次数明显低于算法 1。(4)算法不同对未失效节点的误判次数也不相同，无论网络延迟的设置为多少，算法 2 在实验中对失效的误判率均低于算法 1，特别是当网络延迟越长的情形表现得越明显。

为验证算法 1 和算法 2 对实际上已经失效的进程做出错误判断的情况，在实验中，程序中设置一个计时器，专门记录算法对已经失效进程的判断时间，记录周期为 5ms。两种算法都自动设置进行了 100 次失效检测后，手动结束各节点上的被检测进程，模拟被检测进程已经完全失效。然后手动对两种算法的第 101 次失效进行检测，实验中的数据记录如表 2 所列。

表 2 算法 1 和算法 2 对失效进程的判断时间比较

算法	延迟时间/ms	判断时间 t_Δ/ms
算法 1	2000	480
算法 2	356	62

从表 2 中可知，对于被检测进程已真正失效的情况，算法 1 将过去的误判次数直接转换为下次检测延迟时间的算法，实际增加了延迟时间，造成判断时间的加长；算法 2 在增加了信任度变量和修正比例因子的情形下，能更快判定出已失效进程的状态，提高了检测效率。

结束语 综上所述，本文在对象级、进程级和主机级的层次式失效检测方法的思想指导下，以 Chen 预测算法为基础，通过增设一个信任度变量和修正比例因子，提出了一种分布式系统中的层次式失效检测的改进算法。改进算法考虑到传统的分布式系统中层次式失效检测方法中的单点失效问题和检测时间过长等因素，在分层时考虑了网络拓扑结构，把局域网的检测消息限制在组内，减少了广域网的负载和检测时间；同时，该方法使组内的节点都承担不同组之间检测的任务，从而避免了失效检测系统受单点失效的影响。

实验结果表明，改进后的方法其理论上更趋于合理性，综合及时性与准确性两个标准因素考虑，改进算法能够提高失效检测的准确性和检测效率，其性能优于传统的分布式系统中的层次式失效检测方法。同时，该研究成果也为下一步的优化检测方法研究提供了参考和有用的理论依据。

参 考 文 献

[1] Foster I, Kesselman C, Tuecke S. The anatomy of the grid[J]. Int'l Journal of High Performance Computing Applications, 2001, 15(3): 200-222

[2] Stelling P, Foster I, Kesselman C, et al. A fault detection service for wide area distributed computations [C]// Schmidt D, ed. Proc. of the 7th IEEE Symposium on High Performance Distributed Computing. Chicago: IEEE Computer Society Press, 1998: 268-278

[3] 云晓春，余翔湛. 基于确认度失效检测算法的研究与设计[J]. 北京邮电大学学报，2005，28(3)：10-13

[4] Hayashibara N, Défago X, Yared R, et al. The φ-accrual failure detector[C]// Titsworth FM, ed. IEEE Int'l Symp. on Reliable Distributed Systems (SRDS 2004). Florianopolis: IEEE Computer Society Press, 2004: 66-78

[5] Sotoma I, Madeira E R M. Adaptation—Algorithms to adaptive fault monitoring and their implementation on CORBA [C]// Blair G, Schmidt D, Tari Z, eds. Int'l Symposium on Distributed-objects and Applications (DOA 2001). Rome: IEEE Computer Society Press, 2001: 219-228

[6] 董剑，左德承，刘宏伟，等. 一种基于 QoS 的自适应网格失效检测器[J]. 2006，17(11)：2362-2372

[7] 陈宁江. 面向 Web 服务的层次型动态失效检测体系[J]. 计算机工程，2009，35(17)：94-96

[8] Chen W, Toueg S, Aguilera M K. On the quality of service of failure detectors[J]. IEEE Trans. on Computers, 2002, 51(5): 561-580

[9] 刘鹏. 分布式系统中容错中间件冗余服务的设计与实现[D]. 长沙：中南大学，2009

[10] 栾兰，刘淑芬，张欣佳. 基于检测点失效检测算法的研究与改进[J]. 吉林大学学报，2008，46(4)：681-686