

文章编号:1001-9081(2007)02-0314-04

基于网络全局流量异常特征的 DDoS 攻击检测

罗 华,胡光岷,姚兴苗

(电子科技大学 通信与信息工程学院,四川 成都 610054)

(luohua3713@163.com)

摘 要:由于分布式拒绝服务(DDoS)攻击的隐蔽性和分布式特征,提出了一种基于全局网络的 DDoS 检测方法。与传统检测方法只对单条链路或者受害者网络进行检测的方式不同,该方法对运营商网络中的 OD 流进行检测。该方法首先求得网络的流量矩阵,利用多条链路中攻击流的相关特性,使用 K-L 变换将流量矩阵分解为正常和异常流量空间,分析异常空间流量的相关特征,从而检测出攻击。仿真结果表明该方法对 DDoS 攻击的检测更准确、更快速,有利于 DDoS 攻击的早期检测与防御。

关键词:分布式拒绝服务攻击;全局流量异常;流量矩阵

中图分类号: TP393.08 **文献标识码:** A

DDoS attack detection based on global network properties of network traffic anomaly

LUO Hua, HU Guang-min, YAO Xing-miao

(School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054, China)

Abstract: Due to the invisibility and distributivity characteristics of Distributed Denial of Service (DDoS) attack, a new DDoS detection method based on global network was presented in this paper. Our method detects DDoS by analyzing OD traffic matrix, whereas the traditional methods detect it on single link or victim network. This method was carried out as follows: First, we need to get network traffic matrix in order to obtain the correlation character of attack traffic among multiple links. Then, traffic matrix was divided into normal space and abnormal space by K-L transformation. Finally, the correlation of abnormal space was achieved to detect DDoS attack. The simulation result shows that this proposed method is more accurate and faster than traditional methods. It is in favor of earlier detection of DDoS attack.

Key words: Distributed Denial of Service (DDoS) attack; global network traffic anomaly; Traffic Matrix(TM)

0 引言

分布式拒绝服务(Distributed Denial of Service, DDoS)是指攻击者利用多个计算机对一个或者多个目标分别发起拒绝服务攻击(DoS)。使用客户端/服务器模式,攻击者可以利用许多不知情的计算机作为攻击平台从而成倍地提高拒绝服务攻击效果^[1]。在高速数据包的攻击下,受害者主机的关键资源(带宽、缓冲区、CPU 资源等)迅速耗尽^[2],受害者或者崩溃,或者花大量时间处理攻击包而不能正常服务,给受害者和用户造成严重经济损失,因此有效地检测和防御 DDoS 攻击是构建安全网络的重要组成部分。

传统的 DDOS 检测方式是通过分析流量模型或者数据包特征来检测攻击。如队列模型方法^[3]、客户响应分析法^[4]和单链路的流量信号分析方法^[5]。队列模型方法把服务端的等待队列长度作为检测依据。正常情况下服务器端的等待服务队列比较小,因此用户的请求都能得到及时响应;相反,当受到攻击时等待队列会迅速增大。因此可以对该队列设置一个门限,通过分析等待队列的大小来检测攻击。客户响应分析法利用某些通信协议的拥塞控制机制来检测攻击,如 TCP

协议。服务器在忙时如果收到服务请求,将对该请求延迟响应,正常用户会据此判定网络出现拥塞,通过减小发送窗口大小从而降低请求速率。攻击者作为一个非正常用户,使用虚假 IP 发送数据包,不会收到响应数据包,也就不会降低发送请求速率,因此通过用户的响应特征可以检测出攻击。单条链路的流量信号分析方法是有一条链路的流量信号看作一个一维信号,采用一维信号分析方法进行异常检测(也有个别方法将一维信号分解成二维信号进行分析)。

上述方法能在一定程度上检测 DDoS 攻击,并且在实际应用中取得了好的应用效果。但是随着网络应用的进一步普及,网络流量和服务进一步增加,网络黑客的攻击能力也不断提高,DDoS 攻击对网络的危害进一步增大,上述检测方法也表现出其不足:首先这些方法大都是基于单条链路检测方法,当 DDoS 攻击比较小时,在单条链路上往往并不表现出异常,容易造成漏检;其次上述检测方法大都是集中在受害者网络端的检测,由于 DDoS 攻击的快速性,受害者在检测到攻击后往往来不及做出有效的响应。

本文针对传统检测方法的缺陷,研究全局网络流量矩阵,通过 K-L 变换将流量矩阵分解为正常和异常流量空间,然后

收稿日期:2006-09-04;修订日期:2006-11-09

基金项目:国家自然科学基金资助项目(60572092);四川省青年科技基金资助项目(04ZQ026-028)

作者简介:罗华(1982-),男,四川泸州人,硕士研究生,主要研究方向:计算机通信; 胡光岷(1965-),男,四川眉山人,教授,博士生导师,主要研究方向:通信网与宽带通信技术、网络行为学; 姚兴苗(1976-),男,四川南部人,讲师,博士,主要研究方向:宽带网络、计算机通信网。

分析异常空间流量的相关性来检测DDoS攻击。这种方式将检测位置从受害者网络转移到网络运营商的网络,离攻击源较近,可以尽早检测到DDoS攻击。同时将检测对象从单条链路切换到全局网络,能更加准确地检测出攻击。

1 流量矩阵

流量矩阵描述整个网络各个路径上流量的流动情况,反映整个网络流量的整体概貌,特别是新业务的实时性要求,它为研究人员和管理人员研究和管理网络提供了最直接、最全面的实时信息。流量矩阵的每一行表示网络中一条OD (Origin-Destination)对(或流,或节点)之间的流量,整个流量矩阵描述网络流量在各个OD对间的分布情况。OD节点在这里有更广阔的含义,节点可以是链路(Link)、路由器(Router),也可以是POP(Point-of-Presence)。针对不同的流量工程应用需求,OD节点可以是链路到链路(link-to-link)、路由器到路由器(router-to-router)、POP到POP。相应地,流量矩阵可以是基于链路、路由器或POP的不同流量矩阵,从而满足不同的应用需求。

要获得网络流量矩阵,需要对网络流量进行测量。网络流量的测量种类按测量的协作方式可分为主动测量和被动测量,按测量的情况可分为直接测量和间接测量。由于现有网络设备很少对网络流量的测量提供协作方式,直接对网络流量进行测量将使整个网络付出很大的资源开销,特别是要满足新业务的实时性要求,网络资源开销将会更大,这将大大降低整个网络的性能^[6]。因而,流量矩阵在网络上并不容易直接获得,往往采用被动测量和间接测量为主的方式来获取。

研究人员进行了广泛的研究,提出了流量矩阵估计的各种研究方法。从源节点出发的流通过路由策略被转发到目的地,各个OD流在它所经过的链路上汇聚,而这种汇聚性取决于网络拓扑和路由策略,尽管流量矩阵不容易直接获得,但是各个链路流是很容易通过测量得到的。所以,流量矩阵、路由策略、链路流量之间存在某种关系,这种关系可以由一个线性等式来表示:

$$\mathbf{y} = \mathbf{A}\mathbf{x} \quad (1)$$

其中, \mathbf{y} 是一个列向量,表示链路流量; \mathbf{x} 也是一个列向量,表示流量矩阵; \mathbf{A} 表示路由矩阵, \mathbf{A} 可表示为 $\mathbf{A} = \{a_{ij}\}$, a_{ij} 为矩阵 \mathbf{A} 的元素,如果OD流 j 通过链路 i ,则 $a_{ij} = 1$,否则 $a_{ij} = 0$ ^[7-9]。

一般地,(1)式中的 \mathbf{y} 和 \mathbf{A} 较容易获得, \mathbf{y} 可以通过SNMP测量得到, \mathbf{A} 可以通过路由策略和网络拓扑获得,可见,流量矩阵的求解是一个反问题。但是,由于实际网络中链路测量数远小于OD流数,即 \mathbf{A} 远不是满秩的,故而所面对的问题就是欠定的、病态系统的反问题求解。

2 攻击检测

2.1 OD流的相关性

最新的研究表明网络流量本身具有一定的相关性^[10]。DDoS攻击是由大量攻击源在同一时间段发送相同类型的数据包到同一个目的,由于数据包的类型相同,数据包大小一致,同时由于攻击程序发送攻击包时的规律性,导致攻击流有很强的相关性。为能最大限度地提取出这种相关性,可以用

K-L变换将网络流量分解为正常流量空间和异常流量空间,然后分析异常流量空间的相关性来检测DDoS攻击。

2.2 对流量矩阵的K-L分解

K-L是一种坐标变换方法,它将一组给定的数据映射到一个新的坐标系下。当原始数据列向量是零均值时,变换后的数据将保留原始数据的信息量。在新坐标系下,每个坐标轴携带的信息量从大到小排列。第一个坐标轴携带最大的信息量,第二个坐标轴次之,最后一个坐标轴携带的信息量最小。同时排列在前面很少几个坐标轴携带的信息量占总信息量的很大比例。因此可以考虑用前面几个坐标轴的信息量来重构所有信息量。

对于变换 $\mathbf{Y} = \mathbf{V}\mathbf{X}$,如果 \mathbf{Y} 正交,则 \mathbf{Y} 满足下边的统计特性:

$$E\{[\mathbf{y}_i - E(\mathbf{y}_i)][\mathbf{y}_j - E(\mathbf{y}_j)]^*\} = \lambda_j \delta_{ji} \quad (2)$$

其中:

$$\delta_{ji} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

从(2)式可以看出,当 $i = j$ 时,左边是向量 \mathbf{y}_i 的方差 $var(\mathbf{y}_i)$,右边为常数;当 $i \neq j$ 时,左边是 \mathbf{y}_i 和 \mathbf{y}_j 的协方差 $cov(\mathbf{y}_i, \mathbf{y}_j)$,右边为0。因此 \mathbf{Y} 的协方差矩阵就是一个对角阵 $diag(cov(\mathbf{y}_i, \mathbf{y}_j))$ 。由(2)式可以推出:

$$cov\{\mathbf{X}, \mathbf{X}\} \mathbf{V}_j = \lambda_j \mathbf{V}_j \quad (3)$$

(3)式说明 \mathbf{X} 的协方差矩阵的特征值对应变换后的矩阵 \mathbf{Y} 的方差, \mathbf{X} 的协方差矩阵的特征向量对应变换的正交矩阵,也就是主成分。根据这个对应关系,K-L分解TM矩阵可分为三步:

1) 计算主轴。首先对 \mathbf{X}_{ixm} 的每一列进行零均值化,后边所有提到 \mathbf{X} 的地方都表示 \mathbf{X} 为零均值化后的TM矩阵。然后计算 $\mathbf{X}^T \mathbf{X}$ 的特征值和特征向量,特征值对应 \mathbf{X} 的能量,特征向量对应主轴。按照特征值从大到小的关系排列特征值和特征向量。在重新排列后的主轴中,前面的主轴携带的信息量较大,后边的主轴携带的信息量逐渐减弱。

2) 找出 r 个主轴。为了对TM矩阵进行分解,需要找出 r 个能够代表TM矩阵绝大部分能量的主轴。 r 值的寻找有很多方法,在这里计算 m 个特征值的平均值,如果第 r 个特征值大于平均值,并且第 $r+1$ 个特征值小于平均值,那么这个 r 就是要找的值。

3) 分解流量矩阵。用2)算出的 r 个主成分将流量矩阵分解为正常和异常流量空间。每一个主成分 \mathbf{v}_i 是一个 m 维的向量,这样前面 r 个主成分 $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \dots, \mathbf{v}_r)$ 就构成了一个 $\mathbf{P}_{m \times r}$ 的矩阵。分解流量矩阵就是用 $\mathbf{P}_{m \times r}$ 将时间点 t 的流量分解为正常和异常流量空间。假定 \mathbf{x}_t 是 \mathbf{X} 一个行向量的转置,也就是把 \mathbf{x}_t 分解为正常部分 \mathbf{x}_{t1} 和异常部分 \mathbf{x}_{t2} 两个部分:

$$\mathbf{x}_t = \mathbf{x}_{t1} + \mathbf{x}_{t2} \quad (4)$$

其中:

$$\mathbf{x}_{t1} = \mathbf{P}\mathbf{P}^T \mathbf{x}_t, \mathbf{x}_{t2} = (\mathbf{I} - \mathbf{P}\mathbf{P}^T) \mathbf{x}_t \quad (5)$$

按照时间点顺序把异常空间流量 \mathbf{x}_{t2} 作为一个行向量排列起来就构成了所需的异常空间流量矩阵。

2.3 相关性计算

在下边的计算中,用 O_i 和 O_j 分别表示OD流 i 和OD流 j ;用 T 表示OD流总的采样点数; $cov(i, j, t)$ 表示 O_i 与 O_j 在时间

点 t 上的相关系数;两个时窗 w_1 和 w_2 , w_1 是计算相关系数的向量的大小, w_2 是 w_1 允许滑动的范围,如图 1 所示。

对于两个 OD 流 O_i 和 O_j , 计算它们在时间点 t 上的相关系数 $\text{cof}(i, j, t)$:

$$\text{cof}(i, j, t) = \text{maxcorrcoef}(O_i(t), O_j(t_j)) \quad (6)$$

其中 $\text{maxcorrcoef}(O_i(t), O_j(t_j))$ 是 O_i 在时间点 t , O_j 以时间点 t 为中心, 以 w_2 为半径的时间范围内 OD 流 O_i 和 O_j 的相关系数, 因此(6) 式成立的条件是:

$$\begin{cases} 0 \leq t \leq T - w_1 + 1 \\ t - w_2 \leq t_j \leq t + w_2 \\ i \neq j \end{cases}$$

通过(6) 式, 得到一个 O_i 的连续相关系数序列 $\text{cof}(i, j)$ 。用同样的方法计算其他 OD 流的相关系数。最后计算所有 OD 流相关系数的均值, 得到一个平均相关系数序列 $\text{meancof}(t)$:

$$\text{meancof}(t) = \frac{1}{m} \sum_i \sum_j \text{cof}(i, j, t) \quad (7)$$

其中 $0 \leq t \leq T - w_1 + 1, i \neq j$

通过(7) 式计算出的平均相关系数 $\text{meancof}(t)$, 在后边将对该相关系数设置一个门限, 从而检测 DDos 攻击。

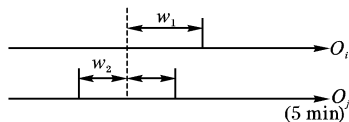


图1 计算相关系数的滑动时窗示意图

2.4 门限设置

为了能准确地检测 DDos 攻击, 需要设置一个门限来判断平均相关系数是否发生了异常。通过对长时间和多个 OD 流的研究发现, 网络流量的相关系数服从正态分布, 如图 2 所示。

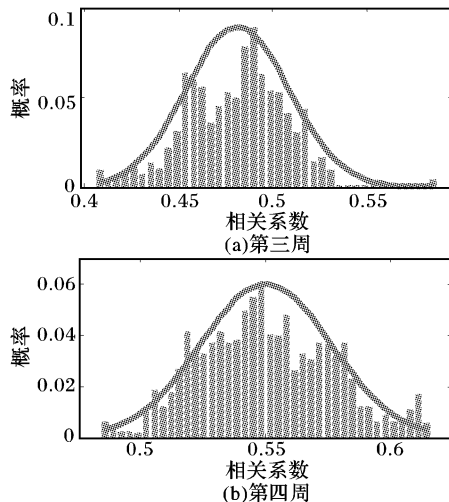


图2 第三周、第四周相关系数分布

因此可以选择一个历史时间段的相关系数的分布情况来设置门限^[11]。假设在这个历史时间段中相关系数的均值为 m , 方差为 δ^2 , 标准差 δ , 门限系数为 α , 门限为 d :

$$d = m + \alpha \times \delta \quad (8)$$

在(8) 式中设置 $\alpha = 2.4$, 置信区间为 $m \pm 2.4\delta$, 等效于检测率可达 99.6% 的置信度, 误报率可以为 0.4%。用这个门限来检验平均相关系数 $\text{meancof}(t)$, 如果:

$$\text{meancof}(t) \geq d$$

那么就认为在时间点 t 上存在 DDos 攻击。

3 仿真

3.1 仿真数据

仿真中用到的 TM 矩阵采至美国 Abilene^[12] 骨干网。它有 12 个节点, 30 条链路。采集时按照 1% 的采样率在每个节点上采集端到端数据, 将每五分钟采集到的数据作为一个时间点, 每周 2016 个时间点。按照这种方式采集了从 2004-03-01 到 2004-09-10 之间总共 24 周的数据。

为检验该方法有效性, 我们在 TM 矩阵中注入攻击流, 这样便于准确地知道“攻击”发生的时间和位置。首先选择受害者节点和相应的 OD 流。在这里随机选择节点 5 作为受害者节点, OD 流 77, 89, 101, 113, 125, 137 为攻击流经过的路径。然后模拟了 8 个 Agent 攻击一台主机的过程, 在受害者入口链路收集数据包, 将每 ms 收集到的数据包总数作为一个时间点, 总共采集 2000ms, 这就构成了一个攻击包序列, 然后对每一个 OD 流, 随机选择该攻击序列中连续的 100 个点作为攻击流注入 OD 流的第 500~600 个时间点中。

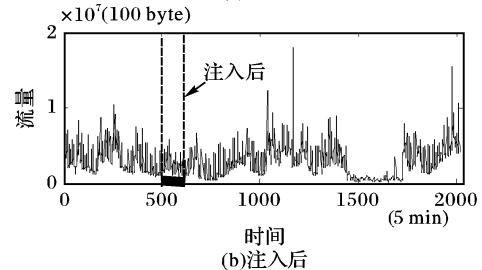
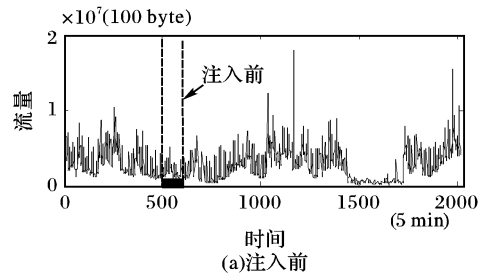


图3 第三周注入前后 OD 流

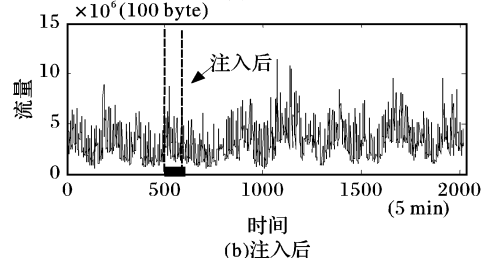
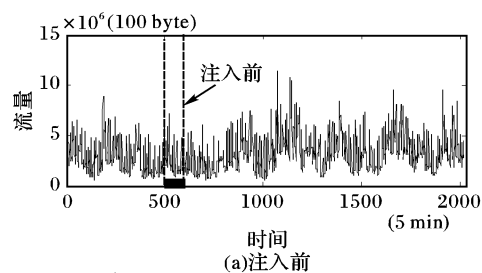


图4 第四周注入前后 OD 流

在后边的仿真中, 我们将用 24 周中的第三周和第四周数据进行说明。图 3 和图 4 中绘制这两周同一个 OD 流注入前后的流量图。通过对这两幅图注入前后流量波形比较可以看

出,采用上边的方式注入的攻击流比较小,这种攻击流可以用来模拟较小的DDoS攻击或者是大规模攻击的早期流量特征。

在具体实现时,在ISP路由节点收集SNMP链路信息,结合拓扑结构和路由信息,计算出OD流的TM矩阵。然后进行K-L变换和相关性异常检测。由于网络中骨干路由节点数目有限,OD流数目相对较小。同时取的时间段小,计算量也就不大,可以做到对异常流量的实时检测。

3.2 仿真结果

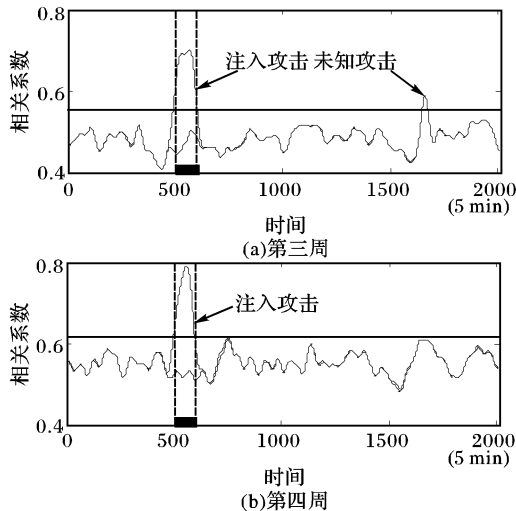


图5 第三周、第四周注入前后的相关系数

在图5中绘制了两周注入攻击流前后流量矩阵的平均相关系数。图中虚线波形是注入前的平均相关系数,实线波形是注入后的平均相关系数。水平线是根据相关系数的正态分布特征设置的门限。从图中可以看出,在攻击流注入的位置500~600之间相关系数出现发生比较剧烈变化,在攻击流注入之外的位置,相关系数重叠。因此,这种方法能很好地提取攻击流的相关性特征,从而准确有效地在ISP网络中检测出较小DDoS攻击。实际的攻击时往往表现为剧烈的流量突变^[13],当检测这样的攻击流时,该方法检测效果更加明显。

4 结语

本文提出了一种基于全局网络的DDoS检测方法,它改变了传统检测方法只能对单条链路或者受害者网络进行检测的方式,在网络营运商的网络中对全局网络中的OD流进行检测。利用K-L变换重构出攻击流,采用双时窗方式,最大限度地找出攻击流的相关性。通过对采集的24周数据的仿真

实验,结果表明该方法能准确快速地检测出攻击强度相对较小的DDoS攻击,为有效防御DDoS攻击和过滤攻击包节约了宝贵的时间。

参考文献:

- [1] STEIN L. The World Wide Web Security FAQ, Version 2.0.1[EB/OL]. <http://www.w3.org/Security/Faq/> - visited, 2000-04-10.
- [2] CHANG RKC. Defending against flooding-based, Distributed Denial of Service attacks: a tutorial[J]. IEEE Communications Magazine. 2002, 40 (10): 42-51.
- [3] HAO S, SONG H, JIANG WB, et al. A Queue Model to Detect DDoS Attacks[A]. Proceedings of the 2005 International Symposium on Collaborative Technologies and Systems[C]. 2005. 106-112.
- [4] SOEJIMA Y, CHEN EY, FUJI H. Detecting DDoS Attacks by Analyzing Client Response Patterns[A]. SAINT Workshops[C]. 2005. 98-101.
- [5] BARFORD P, KLINE J, PLONKA D, et al. A signal analysis of network traffic anomalies [A]. Proceedings of ACM SIGCOMM Internet Measurement Workshop[C]. Marseilles, France, 2002. 71-82.
- [6] PAPAGIANNAKI K, TAFT N, LAKHINA A. A Distributed Approach to Measure Traffic Matrices[A]. In ACM Internet Measurement Conference[C]. Taormina, Italy, October 2004.
- [7] CAO J, DAVIS D, VANDER WEIL S, et al. Time-Varying Network Tomography[J]. Journal of the American Statistical Association, 2000, 95(452): 1063-1075.
- [8] SOULE A, LAKHINA A, TAFT N, et al. Traffic Matrices: Balancing Measurements, Inference and Modeling[A]. ACM Sigmetrics 2005[C]. Banff. June 2005.
- [9] MEDINA A, TAFT N, SALAMATIAN K, et al. Traffic Matrix Estimation: Existing Techniques and New Directions[A]. In ACM SIGCOMM[C]. Pittsburgh, USA, Aug. 2002.
- [10] KIM S, REDDY ALN, VANNUCCI M. Detecting Traffic Anomalies through Aggregate Analysis of Packet Header Data[A]. NETWORKING 2004[C]. 2004. 1047-1059.
- [11] KIM S, REDDY ALN, VANNUCCI M. Detecting Traffic Anomalies at the Source through Aggregate Analysis of Packet Header Data[J]. In Networking, 2004: 1047-1059.
- [12] <http://abilene.internet2.edu/> [EB/OL], 2006.
- [13] BARFORD P, PLONKA D. Characteristics of network traffic flow anomalies[A]. In Internet Measurement Workshop[C]. 2001.

(上接第310页)

参考文献:

- [1] WU T, MALKIN M, BONEH M D. Building intrusion-tolerant application[A]. In: Proceedings of the USENIX Security Symposium [C]. 1999. 79-91.
- [2] SHOUP V. Practical threshold signatures[A]. In: Proceedings of the Eurocrypt 2000. Bruges (Brugge): Springer-Verlag [C]. 2000. 207-220
- [3] FRANKEL Y, GEMMELL P, MACKENZIE PD, et al. . Optimal-Resilience proactive public-key cryptosystems[A]. In: IEEE Symposium on Foundations of Computer Science[C]. 1997. 384-393.
- [4] RABIN T, BEN-OR M. Verifiable secret sharing and multiparty protocols with honest majority[A]. In: Proceedings of the 21st annual ACM Symposium on the Theory of Computing[C]. 1989.
- [5] HERZBERG A, JARECKI S, KRAWCZYK H, et al. . Proactive secret shareing[A]. In: Proc. of CRYPTO[C]. 1995, the 15th Ann. Intl. Cryptology Conf. 1995. 339-352.
- [6] SHAMIR A. How to share a secret[J]. Communications of the ACM. 1979, (22): 612-613.
- [7] 彭蓉, 崔竞松. 门限签名中的部分签名验证协议[J]. 计算机工程, 2005, 31(7): 136-137.