云计算中抗共谋攻击的数据位置验证协议

杜思军,徐尚书,刘俊南,张俊伟,马建峰
(西安电子科技大学网络与信息安全学院,陕西西安 710071)

摘 要: 针对云计算中数据位置验证存在的共谋攻击,本文提出了抗共谋攻击的数据位置验证协议. 首先给出了数据位置验证的系统模型,分析了安全威胁,并给出了数据位置验证的安全定义. 随后,将安全定位协议与数据持有性证明协议相结合,设计了一维空间下的数据位置验证协议,并证明了所提协议满足安全定义且能抵御共谋攻击. 在一维协议基础之上,构建了三维空间下的数据位置验证协议. 最后,在三维空间下将本文所提协议与 Lost 协议和 Geoproof 协议进行了性能的测试和比较. 结果表明所提协议能够验证服务器具体位置且能抵御共谋攻击.

关键词: 云计算; 共谋攻击; 数据位置验证; 安全定位; 数据持有性证明; 数据完整性检验
中图分类号: TN911. 7 **文献标识码:** A **文章编号:** 0372-2112 (2017)06-1321-06
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2017. 06. 006

Collusion-Attack-Defensive Data Location Verification Protocols in Cloud Computing

DU Si-jun, XU Shang-shu, LIU Jun-nan, ZHANG Jun-wei, MA Jian-feng
(*School of Cyber Engineering, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: In view of the collusion attack in cloud computing data location verification, collusion-attack-defensive data location verification protocols are proposed. Firstly, the system model of data location verification is given and the security threats are analyzed and the security definition is formalized. Then, the security positioning protocol is combined with the provable data possession protocol and the data location verification protocol in one dimension is proposed. In addition, the proposed protocol is proved to satisfy the security definition and to defend collusion attack. Based on the proposed protocol, the data location verification protocol in three dimensions is constructed. Finally, in three dimensions, the proposed protocol is tested and compared with the Lost protocol and the Geoproof protocol. The results show the proposed protocol can verify the specific geographical location of the server and can defend collusion attack of the adversaries.

Key words: cloud computing; collusion attack; data location verification; security positioning; provable data possession; position-based cryptography; data integrity check

1 引言

随着云计算不断普及,安全问题重要性呈现逐步上升趋势[1,2]. 一些分析机构调查结果显示,数据安全问题是云计算最大障碍之一[3]. 对于存储位置有特殊要求的数据,在云端存储位置就显得极其重要[4,5]. 比如,欧洲网络和信息安全局及云安全联盟明确将云计算中数据存储位置安全问题列为数据安全的重要问题之一[3~5].

用户为确保数据存储在指定位置,须通过数据位置验证(Data Location Verification, DLV)协议对数据位置和完整性验证. 因此,数据位置验证协议应由两个子协议组成,即地理位置验证协议和数据持有性证明协议. 用户通过 DLV 协议,使在指定位置且保持完整性的数据能通过验证,不在指定位置或在指定位置但完整性被破坏的数据不能通过验证.

目前有四种典型位置验证技术:(1)基于网络技术定位. 典型方法[6~8]有 DNS-LOC 方法、whois 方法及测量 PING 往返时间等,它们主要关注如何用网络中相关协议对网络实体位置进行计算或估计,但不考虑攻击环境下定位的安全问题;(2)基于无线定位. 无线领域定位已有相当多研究成果[9~11],而文献[12]的研究表

收稿日期:2015-10-22; 修回日期:2016-03-23;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61472310, No. U1405255, No. 61372075, No. 61303219, No. 61363068)

明,在此之前的成果不能抵御共谋攻击;(3)距离约束(Distance Bounding,DB)协议[13~15],该协议验证者可判断被验证者是否在一定距离范围内,并不能验证被验证者具体位置;(4)安全定位(Security Positioning,SP)协议[12],该协议将用户位置信息作为唯一凭证,最大特点是能验其具体位置且能抵御共谋攻击.

可证明数据持有[16,17](Provable Data Possession,PDP)和可恢复性证明[18,19](Proof Of Retrievability,POR)均能验证服务器是否正确持有数据,且已有研究成果较为成熟.二者主要区别是:PDP 方案只检测数据完整性;POR 方案在检验完整性同时保证可恢复性.

目前,在数据位置验证协议方面有一系列标志性成果. Geoproof 方案[20]将 DB 协议和 POR 方案相结合,实现数据存储距离的安全验证,但并不能验证 prover 具体位置. Enhanced Geoproof 方案[21]在 Geoproof 基础上使得验证精度更高,但仍不能验证 prover 具体位置. Lost 方案[22]将无线定位技术与 POR 方案结合进行位置验证,但无法抵御共谋攻击.

SP 协议能验证 prover 具体位置,且能抵御共谋攻击.为此,本文将 SP 技术和 PDP 协议[23]结合,构建可证明安全的数据位置验证协议.具体工作如下:

(1)分析敌手攻击模型,给出数据位置验证的安全定义.

(2)设计 1 维空间下的数据位置验证协议.

(3)分析 1 维空间下的数据位置验证协议的安全性.

(4)构建 d ($d\in\{1,2,3\}$)维空间下的数据位置验证协议,比较分析并通过实验测试相关协议性能.

2 系统模型、攻击模型及安全定义

2.1 系统模型

用户需将数据 D 存储在位置 P 的服务器上.在 d($d\in\{1,2,3\}$)维空间,为验证数据 D 的具体位置和完整性,用户雇用验证者 $V=\{V_1,V_2,\cdots,V_K\}$($K\geqslant d+1$).

以 3 维空间为例,系统模型如图 1 所示.用户雇用验证者 V_1、V_2、V_3 和 V_4.用户和 V_1 以及所有验证者之间均存在安全信道.验证者协助用户验证服务器位置,用户验证数据完整性.若服务器位置没有通过验证,则 V_1 直接返回用户 Invalid(P);若服务器位置通过验证,V_1 将服务器响应返回用户,用户对其持有证据进行验证.

2.2 攻击模型

云服务器为降低存储成本,可能不在位置 P 或在位置 P 但破坏了数据完整性.因此,存在共谋敌手 $\mathrm{Adv}=\{A_1,A_2,\cdots,A_K\}$,向用户声称其在位置 P 且持有完整数据 D.

敌手能控制整个网络环境.即能对消息任意窃听、篡改、回放和延迟发送.若敌手在位置 P'($P'\neq P$),或在位置 P 但持有数据为 D'($D'\neq D$).敌手已知位置 P、数据 D 和持有证据算法,从而共谋伪造位置 P' 和数据 D',以此欺骗用户并通过验证.

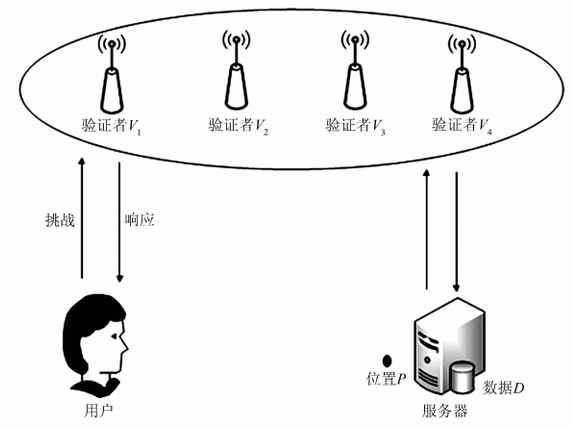

图1 3维空间数据存储位置验证系统模型

2.3 安全定义

令 DLV 为 d($d\in\{1,2,3\}$)维空间下的数据位置验证协议,该协议由两个阶段组成:准备阶段包括 Setup(i),用于计算持有证据 v_i;验证阶段包括产生挑战 Genchal(i)、计算证据 Comver(k_i,c_i)和位置验证 Verify(P,D),用于验证服务器位置和数据完整性.

定义 1 用户将数据 D 存储在位置 P 的服务器,对任意 PPT(Probabilistic Polynomial Time)共谋敌手为 $\mathrm{Adv}=\{A_1,A_2,\cdots,A_K\}$,给定敌手 A_i($1\leqslant i\leqslant K$)持有证据算法 Comver(k_i,c_i)、位置 P 和数据 D.若选择安全参数 κ,敌手 A_i 能成功伪造位置 P' 和数据 D'($P'=P$ 且 $D'\neq D$ 或 $P'\neq P$)的概率可忽略,则称协议 DLV 是安全的,即

$$\mathrm{Prob}[(P',D')\leftarrow A_i^{\mathrm{Comver}(k_i,c_i)}(P,D):P'=P,\ D'\neq D\mid P'\neq P,\mathrm{Verify}(P',D')=1]\leqslant\varepsilon(\kappa) \tag{1}$$

3 预备知识

3.1 BRM 模型

BRM(Bounded Retrieval Model)模型假设所有敌手只检索具有高最小熵(high min-entropy)信息的一部分.具体如下:

①验证者可生成熵值为$(\delta+\beta)n$ 的 n 比特串 X.

②当 X 经过时,所有敌手都可检索 X 的任何部分,但是检索总信息量不超过上限 βn.

3.2 BSM 伪随机生成器

PRG $F:\{0,1\}^n\times\{0,1\}^r\rightarrow\{0,1\}^t$ 是 ε-secure 的 BSM 伪随机生成器(BSM Pseudorandom Generator,BSM PRG),当且仅当对 $\{0,1\}^n$ 上任意 αn-source 的 X,对任意 $A:\{0,1\}^n\rightarrow\{0,1\}^{\beta n}$,随机变量(PRG($X$,$K$),$A$($X$),

K)对(W,$A(X)$,K)是 ε-close 的,其中 K 为$\{0,1\}^r$ 上随机数,W 是 ψ-source 的.

选择安全参数 κ,如果 $r \geqslant (2/\delta)\kappa\mathrm{lb}(n)$,则 $\varepsilon + 2^{-\psi}$可忽略. 在 BRM 模型下,若选择合适 r,敌手能正确计算 PRG(X,K)的概率可忽略.

4　1 维空间下的数据位置验证协议(DLV ^{1})

4.1　准备阶段

用户将数据 D 分成 d 个大小相等数据块 $D_{[1]},\cdots,D_{[d]}$. 验证次数为 t,持有证据中数据块数为 m. 选择参数 c,l,k,L 及密钥 W,Z,$K\in\{0,1\}^k$,并将伪随机函数 f 和伪随机变换 g 定义如下:

$$f:\{0,1\}^c\times\{0,1\}^k\to\{0,1\}^L$$
$$g:\{0,1\}^l\times\{0,1\}^L\to\{0,1\}^l$$

用户产生 t 个挑战并计算相应的持有证据. 第 i 个持有证据的算法如下:

(1) 用户产生变换密钥 $k_i=f_W(i)$ 和挑战 $c_i=f_Z(i)$;

(2) 计算持有证据中所含数据块 $I_j=g_{ki}(j)$,其中 $I_j\in[1,\cdots,d]$ 且 $1\leqslant j\leqslant m$;

(3) 计算持有证据 $v_i=H(c_i,D_{[I_1]},\cdots,D_{[I_m]})$;

用户计算出 t 个持有证据,并用私钥 K 将其加密:$v_i'=\mathrm{AE}_K(i,v_i)$,而后将$\{D,[i,v_i']\}$发送给服务器.

4.2　验证阶段

用户和 V_1 及 V_1 和 V_2 之间均存在安全信道. 第 i 个位置验证算法如下:

(1)产生挑战

用户产生(k_i, c_i),即 $k_i=f_W(i)$ 和 $c_i=f_Z(i)$,并将[k_i, c_i]发给 V_1.

(2)计算证据

①设消息从 V_1、V_2 传到 P 点所需时间分别为 t_1 和 t_2. V_1 选取随机数 r_1 和 s_1,并将(r_1,s_1)和(k_i, c_i)发给 V_2. V_2 选取随机串 X_1 和 Y_1,并计算 $r_2'=\mathrm{PRG}(X_1,r_1)\oplus k_i$ 和 $s_2'=\mathrm{PRG}(Y_1,s_1)\oplus c_i$;

②在($T-t_1$)时刻 V_1 发送 r_1 和 s_1,在($T-t_2$)时刻 V_2 发送(X_1,r_2')和(Y_1,s_2'). 在时刻 T,服务器计算 $r_2=\mathrm{PRG}(X_1,r_1)\oplus r_2'$ 和 $s_2=\mathrm{PRG}(Y_1,s_1)\oplus s_2'$;

③服务器计算持有证据:$z=H(s_2,D[g_{r2}(1)],\cdots,D[g_{r2}(m)])$;

④服务器发送[z, v_i']给 V_1 和 V_2;

(3)验证数据位置

(ⅰ)若 V_1 和 V_2 收到响应的时刻分别为($T+t_1$)和($T+t_2$),则 V_1 将服务器响应[z,v_i']返回给用户. 用户对 v_i' 解密:$v_i=\mathrm{AE}_K^{-1}(v_i')$.

①若 $z=v_i$,则通过验证.

②若 $z\neq v_i$,则未通过验证.

(ⅱ)若 V_1 收到响应的时刻不是($T+t_1$),或 V_2 收到响应的时刻不是($T+t_2$),则 V_1 返回用户 Invalid(P),说明服务器不在位置 P,则不能通过验证.

4.3　安全性分析

定理 1　若 H 是单向哈希函数,F 是 ε-secure BSM PRG,则协议 DLV^1 在共谋攻击下满足数据位置验证的安全定义.

假设协议 DLV^1 不满足数据位置验证安全定义,则敌手能伪造位置 P' 和数据 D',$P'\neq P$ 且 $D'\neq D$ 或 $P'\neq P$,使得通过验证概率不可忽略,即:

$$\begin{aligned}&\mathrm{Prob}[(P',D')\leftarrow A_i^{\mathrm{Comver}(k_i,c_i)}(P,D):P'=P,\\&D'\neq D\mid P'\neq P,\mathrm{Verify}(P',D')=1]\geqslant\varepsilon(\kappa)\end{aligned}\tag{2}$$

因此,定理 1 可归以下两个引理来证.

引理 1　若 H 是单向哈希函数,当 $\mathrm{apos}_i=P(1\leqslant i\leqslant k)$且 $D_i\neq D$ $(1\leqslant i\leqslant k)$时,敌手 A_i 能通过验证的概率可忽略. 即:

$$\begin{aligned}&\mathrm{Prob}[(P',D')\leftarrow A_i^{\mathrm{Comver}(k_i,c_i)}(P,D):P'=P,\\&D'\neq D,\mathrm{Verify}(P',D')=1]\leqslant\varepsilon_1(\kappa)\end{aligned}\tag{3}$$

证明　若敌手以不可忽略概率 ε_1 来计算证据 z' 并通过验证. 敌手 A_i 在位置 P,则在时刻 T 能同时收到 V_1 和 V_2 发送的消息,能正确计算出挑战(k_i, c_i),且计算出 z' 后能及时返回 V_1 和 V_2.

若服务器修改了 n 个数据块,则敌手伪造出证据 z' 且能通过验证概率为:$P_1=\frac{d-n}{d}\cdot\frac{d-1-n}{d-1}\cdot\frac{d-2-n}{d-2}\cdots\frac{d-m+1-n}{d-m+1}$经放缩可得到:

$$\left(\frac{d-m+1-n}{d-m+1}\right)^m\leqslant p_1\leqslant\left(\frac{d-n}{d}\right)^m\tag{4}$$

由式(4)可知,敌手 A_i 伪造 z' 且能通过验证最大概率为 $p_1=\left(\frac{d-n}{d}\right)^m$.

若存在敌手 A_H,能伪造 z' 并通过验证,则 $z'=z$,必有 A_H 攻破单向哈希函数的概率为:

$$\varepsilon_H=\varepsilon_1-\left(\frac{d-n}{d}\right)^m\tag{5}$$

因为 ε_1 不可忽略,选择适当参数,$\left(\frac{d-n}{d}\right)^m$ 是可忽略的,则 ε_H 不可忽略,这与单向哈希函数定义相矛盾. 所以 ε_1 可忽略,即引理 1 得证.

引理 2　若 F 是 ε-secure BSM PRG,当 $\mathrm{apos}_i\neq P(1\leqslant i\leqslant k)$时,敌手 A_i 能通过验证的概率可忽略,即:

$$\begin{aligned}&\mathrm{Prob}[(P',D')\leftarrow A_i^{\mathrm{Comver}(k_i,c_i)}(P,D):P'\neq P,\\&\mathrm{Verify}(P',D')=1]\leqslant\varepsilon_2(\kappa)\end{aligned}\tag{6}$$

证明　若存在共谋敌手 $\mathrm{Adv}=\{A_1,A_2,\cdots,A_k\}$,且

敌手均不在位置 P.

若在 V_2 和 P 之间存在共谋敌手. 令 q 表示敌手存储的信息集合,则 $q=q_1\cup q_2\cup\cdots\cup q_g$. 很显然,$|q|\leqslant\beta n$. 对任意算法 F,给定 $A(X)$ 和 K,$F(A(X),K)$ 能正确计算 $\mathrm{PRG}(X,K)$ 的最大概率为 $\varepsilon+2^{-\psi}$,其中 $2^{-\psi}$ 可忽略. 所以,位于 V_2 和 P 之间的敌手计算出 $\mathrm{PRG}(X_1,r_1)$ 和 $\mathrm{PRG}(Y_1,s_1)$ 且能在 $(T+t_2)$ 时刻返回 V_2 的概率可忽略.

若在 V_1 和 P 之间存在共谋敌手. 敌手均能存储 r_1,s_1. 敌手虽能正确计算出 $\mathrm{PRG}(X_1,r_1)$ 和 $\mathrm{PRG}(Y_1,s_1)$,但返回 V_2 的时间要晚于 $(T+t_2)$. 因此,V_1 和 P 之间的敌手不能通过验证.

若存在敌手 A_F,能以不可忽略概率 ε_2 来计算 z' 使得通过验证. 则敌手必以不可忽略概率计算 $[k_i,c_i]$. 则敌手 A_F 攻破 BSM PRG 伪随机性的概率:

$$\varepsilon_F=\varepsilon_2-2^{-\psi} \tag{7}$$

ε_2 不可忽略,$2^{-\psi}$ 可忽略,则 ε_F 也不可忽略. 这与 ε-secure 的 BSM PRG 定义相矛盾. 因此,ε_2 可忽略,即引理 2 得证.

由引理 1 和引理 2 知,当服务器在位置 P 但不持有数据 D,或不在位置 P,通过验证概率为:

$$\varepsilon=\varepsilon_1+\varepsilon_2=\varepsilon_H+\varepsilon_F+2^{-\psi}+\left(\frac{d-m+1-n}{d-m+1}\right)^m \tag{8}$$

若 H 是单向哈希函数,F 是 ε-secure BSM PRG,ε_H 和 ε_F 都可忽略,选择合适参数 κ,$2^{-\psi}$ 和 $\left(\frac{d-m+1-n}{d-m+1}\right)^m$ 均可忽略,所以 ε 可忽略,即定理 1 得证.

4.4 抵御共谋攻击分析

若存在共谋敌手 $\mathrm{Adv}=\{A_1,A_2,\cdots,A_K\}$,均能对用户和 V 发送的消息窃听、篡改、回放和延迟发送等操作.

如果敌手不在位置 P. 若 g 个敌手位于 V_2 和 P 之间,这 g 个敌手存储的随机串分别记为 $q_1,q_2,\cdots,q_g$. 令 q 表示敌手存储的信息集合,则 $q=q_1\cup q_2\cup\cdots\cup q_g$. 因 r_1,s_1 在时刻 T 未到达 P 点,q 只是 X_1、Y_1 的一部分,则敌手不能计算出 (k_i,c_i),从而不能计算出证据来通过验证. 若 g 个敌手在 V_1 和 P 之间,则能存储 r_1,s_1,可计算出 (k_i,c_i),但返回 V_2 的时间要晚于 $(T+t_2)$,则不能通过验证.

如果 g 个共谋敌手在位置 P 但持有数据为 D' $(D'\neq D)$,此时能正确计算出 (k_i,c_i),而敌手计算的持有证据为 z',要使 $z'=z$,必有敌手能攻破单向哈希函数,这与单向哈希函数的定义相矛盾.

综上所述,本文提出的数据位置验证协议能抵御共谋攻击.

5 协议扩展与性能分析测试

5.1 d 维空间下的数据位置验证协议

将 DLV^1 协议扩展至 $d(d\in\{1,2,3\})$ 维空间,构建 d 维空间下的数据位置验证协议 DLV^d.

DLV^d 协议的准备阶段及验证阶段产生挑战和位置验证方法与 DLV^1 协议均相同,不同的是服务器持有证据的

计算. 第 i 个挑战的证据计算如下:

①V_1 将 (r_1,s_1) 和 (k_i,c_i) 发给 $V_j(2\leqslant j\leqslant d+1)$. V_j 选 X_{j-1} 和 Y_{j-1},并计算 $r_j'=\mathrm{PRG}(X_{j-1},r_1)\oplus k_i$ 和 $s_j'=\mathrm{PRG}(Y_{j-1},s_1)\oplus c_i$.

②在 $(T-t_1)$ 时刻 V_1 发 r_1 和 s_1 给服务器,在 $(T-t_j)$ 时刻 V_j 发 (X_{j-1},r_j') 和 (Y_{j-1},s_j') 给服务器.

③在时刻 T,服务器计算 $r_j=\mathrm{PRG}(X_{j-1},r_1)\oplus r_j'$,$s_j=\mathrm{PRG}(Y_{j-1},s_1)\oplus s_j'$ 和 $z=H(s_j,D[g_{rj}(1)],\cdots,D[g_{rj}(m)])$,并将响应 (z,v_i') 发给 V_j.

定理 2 如果 H 是单向哈希函数,F 是 ε-secure BSM PRG,则协议 DLV^d 在共谋攻击下满足数据位置验证的安全定义.

定理 2 证明与定理 1 相似,此处不再赘述.

5.2 性能分析

大多数数据位置验证和持有性证明协议进行性能比较的主要指标是计算代价和通信开销[24]. 因此将 DLV 协议与具有代表性的 Geoproof 协议和 Lost 协议比较,分析和比较各协议通信开销、计算代价、定位技术、是否抵抗共谋攻击等. 比较结果如表 1 所示.

由表 1 看出:Geoproof 协议采用 DB 定位技术,计算低价和通信开销最小,但不能验证服务器具体位置,且不能抵御共谋攻击;Lost 协议采用无线定位技术,计算代价和通信开销也较小,但仍不能抵御共谋攻击;而 DLV 协议采用 SP 定位技术,虽增加计算代价和通信开销,但能验证服务器具体位置且能抵御共谋攻击.

表 1 DLV 协议与 Lost 协议和 Geoproof 协议的性能比较结果

协议			DLV	Lost	Geoproof
计算代价	准备阶段		$2tR+tmP+tH+tE$	$nR+nH+2E$	$1E+1P+nH$
	验证阶段	验证者	$6R+6F+1E^{-1}$	$2e+nH$	$k\lvert\Delta t\rvert+1H$
		服务器	$2F+mP+1H$	$e+1H$	$\lvert\Delta t_{lj}\rvert$
通信开销		验证者	$6\lvert X_i\rvert+6\lvert r_i'\rvert+2\lvert r_1\rvert$	$\lvert T_\rho\rvert$	$\lvert c_j\rvert$
		服务器	$\lvert z\rvert+\lvert v_i'\rvert$	$\lvert\mu_j\rvert+\lvert\sigma_\rho\rvert$	$\lvert s_i\rvert$
定位技术			SP	无线定位	DB
抵抗共谋攻击			√	×	×
支持数据动态更新			×	×	×

在表 1 中,R 表示一次 PRF 计算;F 表示一次 BSM 模型的 PRG 计算;P 表示一次 PRP 计算;H 表示一次哈希运算;E 表示一次加密计算;E^{-1} 表示一次解密计算;e 表示一次双线性映射计算,$|\Delta t|$ 表示一次时间差.

5.3 性能测试

通过实验,测试 DLV 与 Lost 和 Geoproof 协议的计算代价. 实验时,不考虑信息传输时延. 本机硬件环境:双核 i3CPU,4GB 内存;软件环境:win7 系统,java 语言.

选取参数:$D=1\text{MB}$,$d=2^{16}$,$t=16$,$c=\log 16=4$,$l=\log 2^{16}=16$,$k=128\text{bit}$,$L=128\text{bit}$,$m=10$,X 和 Y 选取为 2MB. 进行十六次实验测试.

如图2 所示:在云服务器上存储相同大小数据,Geoproof 协议总的计算代价最小,Lost 协议次之,DLV 协议较大. 与 Geoproof 和 Lost 协议相比,DLV 协议明显增强协议安全性. 从安全性和效率这两个指标看,若用户更关注协议安全性,或在共谋攻击环境下,本文所提 DLV 协议更适合.

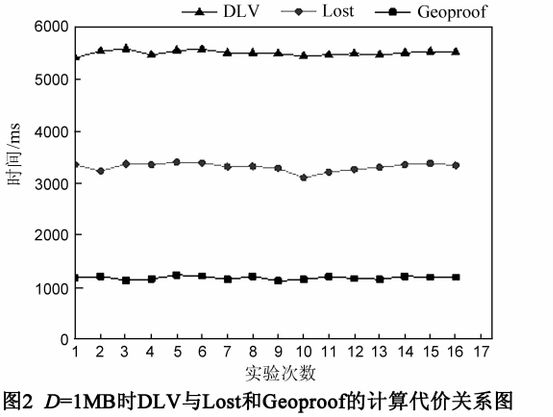

图2 D=1MB时DLV与Lost和Geoproof的计算代价关系图

6 结论

本文在共谋攻击模型下给出了数据位置验证的安全定义. 随后,设计了 1 维空间下的数据位置验证协议,并分析了其安全性. 在此基础之上,提出了 $d(d\in\{1,2,3\})$维空间下的数据位置验证协议. 最后,与相关协议进行了性能比较、分析和测试. DLV 协议与其它协议相比,虽增加计算代价和通信开销,但能验证服务器具体位置且能抵御共谋攻击.

参考文献

[1] 俞能海,郝卓,徐甲甲,等. 云安全研究进展综述[J]. 电子学报,2013,41(2):371 – 381.
Yu N,Hao Z,Xu J,et al. Review of cloud computing security [J]. Acta Electronica Sinica,2013,41(2):371 – 381. (in Chinese)

[2] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22(1):71 – 83.
Feng D G,Zhang M,Zhang Y,et al. Study on cloud computing security[J]. Journal of Software,2011,22(1):71 – 83. (in Chinese)

[3] Zissis D,Lekkas D. Addressing cloud computing security issues[J]. Future Generation Computer Systems,2012,28(3):583 – 592.

[4] Brunette G,Mogull R. Security guidance for critical areas of focus in cloud computing v2.1[J]. Cloud Security Alliance,2009(11). 1 – 76.

[5] Takabi H,Joshi J B D,Ahn G J. Security and privacy challenges in cloud computing environments[J]. IEEE Security & Privacy,2010 (6):24 – 31.

[6] Gueye B,Ziviani A,Crovella M,et al. Constraint-based geolocation of internet hosts[J]. IEEE/ACM Transactions on Networking,2006,14(6):1219 – 1232.

[7] Gill P,Ganjali Y,Wong B,et al. Dude,where's that IP? circumventing measurement-based IP geolocation[A]. Proceedings of the 19th USENIX Conference on Security[C]. USA:USENIX Association,2010. 16 – 31.

[8] Katz-Bassett,Ethan,et al. Towards IP geolocation using delay and topology measurements[A]. Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement [C]. USA:ACM,2006. 71 – 84.

[9] Zeng Y,Cao J,Hong J,et al. Secure localization and location verification in wireless sensor networks[A]. IEEE 6th International Conference on Mobile Adhoc and Sensor Systems,2009(MASS'09)[C]. USA:IEEE,2009. 864-869.

[10] Chiang J T,Haas J J,Choi J,et al. Secure location verification using simultaneous multilateration[J]. IEEE Transactions on Wireless Communications,2012,11(2):584 – 591.

[11] Zhu Y,Ma D,Huang D,et al. Enabling secure location-based services in mobile cloud computing[A]. Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing[C]. USA:ACM,2013. 27 – 32.

[12] Chandran N,Goyal V,Moriarty R,et al. Position based cryptography [A]. Advances in Cryptology-CRYPTO 2009[C]. Berlin:Springer-Verlag,2009. 391 – 407.

[13] Cremers C,Rasmussen K B,Schmidt B,et al. Distance hijacking attacks on distance bounding protocols[A]. 2012 IEEE Symposium on Security and Privacy (SP)[C]. USA:IEEE,2012. 113 – 127.

[14] Rasmussen K B,Capkun S. Realization of RF distance bounding[A]. Proceedings of the 19th USENIX Conference on Security[C]. USA:USENIX Association,2010. 389 – 402.

[15] Hancke G P,Kuhn M G. Attacks on time-of-flight distance bounding channels [A]. Proceedings of the first ACM Conference on Wireless Network Security [C]. USA:ACM,2008. 194 – 202.

[16] Erway C,Kupcu A,Papamanthou C,et al. Dynamic provable data possession[A]. Proceedings of the 16th ACM Conference on Computer and Communications Security

[C]. USA:ACM,2009. 213 – 222.
[17] Zhu Y,Wang H,Hu Z,et al. Efficient provable data possession for hybrid clouds[A]. Proceedings of the 17th ACM Conference on Computer and Communications Security[C]. USA:ACM,2010. 756 – 758.
[18] Bowers K D,Juels A,Oprea A. Proofs of retrievability:Theory and implementation[A]. Proceedings of the 2009 ACM Workshop on Cloud Computing Security[C]. USA:ACM,2009. 43 – 54.
[19] Zhu Y,Wang H X,Hu Z X,et al. Zero-knowledge proofs of retrievability[J]. Science China Information Sciences,2011,54(8):1608 – 1617.
[20] Albeshri A,Boyd C,Nieto J G. Geoproof:proofs of geographic location for cloud computing environment[A]. 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)[C]. USA:IEEE,2012. 506 – 514.
[21] Albeshri A,Boyd C,Nieto J G. Enhanced GeoProof:improved geographic assurance for data in the cloud[J]. International Journal of Information Security,2014,13(2):191 – 198.
[22] Watson G J,Safavi-Naini R,Alimomeni M,et al. Lost:location based storage[A]. Proceedings of the 2012 ACM Workshop on Cloud Computing Security Workshop[C]. USA:ACM,2012. 59 – 70.
[23] Ateniese G,Di Pietro R,Mancini L V,et al. Scalable and efficient provable data possession[A]. Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks[C]. USA:ACM,2008. 1 – 10.
[24] 陈兰香,许力. 云存储服务中可证明数据持有及恢复技术研究[J]. 计算机研究与发展,2012(S1):19 – 25.
Lanxiang C,Li X. Research on provable data possession and recovery technology in cloud storage[J]. Journal of Computer Research and Development,2012(S1):19 – 25. (in Chinese)

作者简介

杜思军 男,1983 年生于湖北襄阳. 现为西安电子科技大学硕士研究生,主要研究方向为网络与信息安全.
E-mail:617021248@qq.com

徐尚书 男,1992 年生于重庆. 现为西安电子科技大学硕士研究生,主要研究方向为无线网络安全.
E-mail:278567131@qq.com

刘俊南 男,1991 年生于广东揭西. 现为西安电子科技大学硕士研究生,主要研究方向为网络与信息安全.
E-mail:1457870709@qq.com

张俊伟 男,1982 年生于陕西西安. 现为西安电子科技大学副教授,硕士生导师,主要研究方向为网络与信息安全、密码学等.
E-mail:jwzhang@xidian.edu.cn