Journal of Computer Applications
计算机应用,2013,33(9):2516 -2519,2524
ISSN 1001-9081
CODEN JYIIDU
2013-09-01
http://www.joca.cn

文章编号:1001-9081(2013)09-2516-04
doi:10.11772/j.issn.1001-9081.2013.09.2516

# 车载网络中隐私保护方法

崔丽群*,张明杰
(辽宁工程技术大学 软件学院,辽宁 葫芦岛 125105)
(*通信作者电子邮箱 zhangmj_keda@163.com)

**摘　要**:针对车载网络通信中存在车辆隐私性保护问题,提出一个*K*-匿名链隐私保护机制。在查询节点处构建*k*匿名空间,并将包含此*k*个车辆的最小边界矩阵作为位置数据进行转发,转发过程中构造一条匿名链来混淆身份信息与位置信息的一一对应关系,从而大大降低被攻击成功的概率。通过对该机制安全性及仿真实验结果的分析,该机制能很好地保护车载网络中车辆的位置隐私,提高了车载网络通信的安全性及隐私性。

**关键词**:位置隐私;匿名空间;*K*-匿名链;Chord;车载网络
**中图分类号**:TP393.08　　**文献标志码**:A

# Privacy protection method in vehicular networks

CUI Liqun*, ZHANG Mingjie
(*College of Software, Liaoning Technical University, Huludao Liaoning* 125105, *China*)

**Abstract:** Concerning the privacy protection problem in Vehicular Ad Hoc NETwork (VANET), a scheme based on *K*-anonymous chain privacy protection was proposed. The scheme built a *k* anonymous area near the query node and forwarded the minimum boundary rectangle containing the *k* vehicles as location data. The process of forwarding constructed an anonymous chain to confuse the corresponding relationship of identity information and location information, thus greatly reducing the probability of successful attack. Seen from the analysis of security and simulation experiment results, this scheme can well protect the privacy of mobile vehicles and improve the security and privacy of vehicular network communication.

**Key words:** location privacy; anonymous space; *K*-anonymous chain; Chord; vehicular network

## 0　引言

车载网络(Vehicular Network)指的是依赖于能够灵活移动的载具而存在的移动自组织网络(Ad Hoc Network),它创造性地将自组织网技术应用于车辆间通信,使司机能够在超视距的范围内获得其他车辆的状况信息(如车速、方向、位置、刹车板压力等)、实时路况[1]及本地化的服务信息[2]。车载网络的特点是网络节点非常多,成员分布区域广,流动性大,车载网络的信息发送本质上是以广播的形式发送,同时由于车辆网络的相对局部性,车载网络中网络节点之间的建立的关系往往持续时间非常短,网络拓扑变化非常快。基于以上特点,车载网络非常容易受到安全攻击,而且相对来说,车载网络对网络安全性攻击是非常敏感的,车载网络的安全性直接关系到车辆驾驶的交通安全性。所以在部署车载网络的过程中,车载网络的安全性必须得到充分的保障。

随着车载网络服务的不断发展,在道路交通变得更加便利的同时,车载网络中车辆隐私性保护问题越来越受到关注。如果允许第三人利用车载网络收集车辆行驶信息,驾驶员的个人隐私必定会受到侵害。所以隐私性保护是车载网络中非常重要的问题。对于隐私性保护在车载网络中的研究,目前已经有很多研究方案:利用群签名的方案[3]、基于ID的签名的方案[4]、基于假名的签名方案[5]、假数据方案[6]、基于空间变换的匿名方案[7]、基于匿名链的位置隐私保护方案[8]等。其中,假名签名方案已经得到一定范围的认可,但大多数假名签名方案都采用预置一定数量的假名,每个假名仅使用一段时间就更换,使用完后需要向证书授权机构(Certificate Authority, CA)请求一组新的假名,这在降低效率的同时大大增加了窃听的概率;基于匿名链的位置隐私保护方案只是隐藏了身份信息和位置息的关联关系,保留了精确的位置数据,这就大大增加了被恶意攻击者攻击成功的概率。

本文所讨论的车载网络指的是狭义上的车载网络,即完全由交通车辆形成的车载网络。主要针对车载网络中车辆间的网络通信隐私性保护问题,提出一种新的*K*-匿名链隐私保护机制,以增强车载网络通信的隐私性及安全性。

## 1　轨迹隐私保护中相关定义

为了能够更好地理解*K*-匿名链机制,先来了解一下*K*-匿名链机制中涉及到的一些定义。

**定义1**　发送者节点。发送者节点是指根据自身对匿名质量要求发起匿名查询的移动车辆。

**定义2**　转发节点。转发节点是指那些能够帮助发起者建立匿名链的移动车辆,转发节点可以将包含发送者的*K*-匿名空间连同查询请求在匿名链中进行转发。

**定义3**　接收者节点。接收者节点是匿名链的终点移动车辆,它最终将转发信息提交给基于位置的服务(Location-Based Service, LBS)服务器。

**定义4**　空间*K*-匿名。假设*S*是任意*k*个不同身份的车辆实体组成的集合,如果车辆*u*是*S*中的一个子集,在包含空间

**收稿日期**:2013-03-27;**修回日期**:2013-05-01。　**基金项目**:国家自然科学基金资助项目(61172144)。
**作者简介**:崔丽群(1969 -),女,天津人,副教授,主要研究方向:嵌入式系统、软件工程;　张明杰(1987 -),男,山东临沂人,硕士研究生,主要研究方向:嵌入式系统、Ad Hoc网络。

$k$ 个用户的最小空间匿名区域中,$u$ 被识别出的概率不超过 $1/k$,则称对 $u$ 实现了 $K$- 匿名。

**定义 5**　隐私。隐私是指个人、机构等实体不愿意被外部所获知的信息。

**定义 6**　连通性。连通性是移动车辆通信的最大距离与两个移动车辆间的距离的比值,记作 $St = d/R$。其中:$d$ 表示在 $t$ 时刻两移动车辆间的距离,$R$ 为移动车辆通信的最大距离。

## 2　$K$-匿名链机制

### 2.1　希尔伯特算法

在车载网络中 $K$-匿名链机制采用希尔伯特空间填充曲线将移动车辆所在的二维空间位置坐标映射为按关键字大小排列的一维序列,然后移动车辆根据扩展能力好、容错性高的 Chord 分布式哈希表结构[10] 自组织到一个车载网络系统中,构成一个 Chord 环的结构。Chord 环上的节点为簇头节点,Chord 环是由这些簇头节点及其前驱和后继节点组成。本文设定 Chord 环上的节点不是单个用户而是一簇用户,簇中成员节点及其信息由簇头节点维护,并负责 $K$-匿名空间的构建。

车载网络中的车辆具有很强的移动性[9],车辆的加入或者离开会导致簇中节点的数量的改变,这就要求簇中节点数量不能无节制地增加或者减少。文中采用每个簇有 $a$ 到 $3a$ 个车辆,其中 $a$ 是个系统参数。如果簇中节点数达到 $3a$,将执行分裂而形成另一个环;如果小于 $a$,将会和另一个 Chord 环上节点融合形成一个簇。

假设 $[U_1, U_2, \cdots, U_n]$ 是所有车辆根据希尔伯特空间算法得到的一维序列,经 Chord 分布式协议将这一序列构成一个首尾相连的 Chord 环,如图 1 所示。

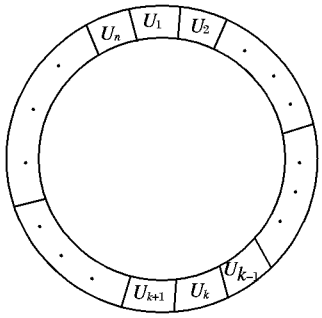


图 1　Chord 环结构

### 2.2　$K$-匿名链

为了解决车载网络环境中的隐私性保护问题,徐建等[8] 提出基于匿名链的位置隐私保护方法,但是这种方法只是隐藏了身份信息和位置信息的关联关系,保留了精确的位置数据,无法满足高匿名性的要求。为了解决这个问题,本文提出一种 $K$-匿名链机制,主要由两部分组成:移动车辆和 LBS 服务器。移动车辆可分为发送者节点、转发节点和接收者节点。发送者节点先构建 $K$-匿名空间,并将此匿名空间连同查询信息一起发送到转发节点上形成一条通向接收者匿名链,由接收者向 LBS 服务器[11] 发起查询,经 LBS 服务器处理得到的候选结果集直接发送给发送者,由移动车辆对候选结果进行求精。图 2 表示 $K$-匿名链机制原理。

图 2 中 Chord 环上的节点(AD1 ~ AD6)称为簇头节点,其中 AD2、AD6 分别为 AD1 的后继和前驱节点,S 代表发送者节点,R 代表接收者节点,整个 Chord 环就是由簇头节点及其前驱或后继节点构成。在上文中已经提及到,Chord 环上的节点

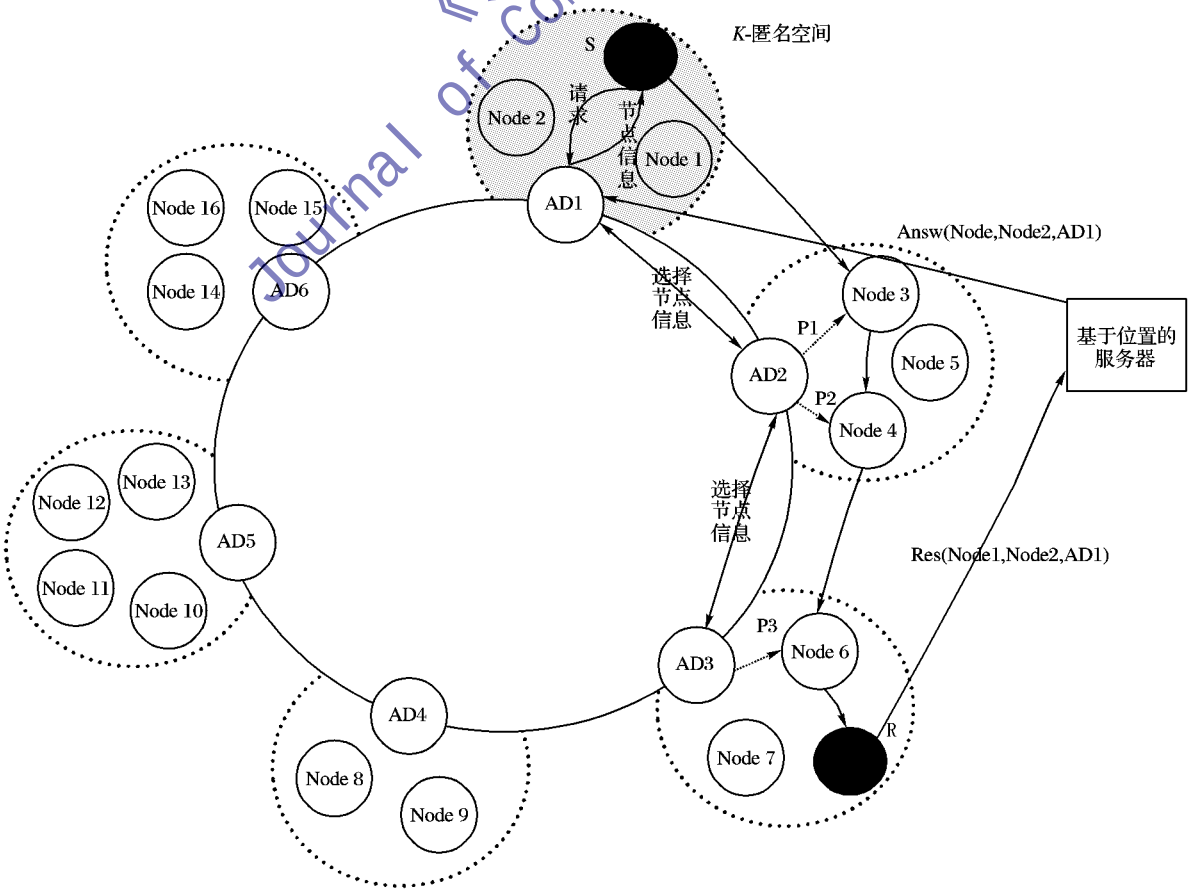


图 2　$K$-匿名链机制

并不代表单一用户,而是表示了一簇车辆,例如以 AD2 为簇头节点的簇包含 Node3、Node4、Node5 三个簇成员。

### 2.2.1 *K*-匿名请求

*K*-匿名请求过程中,发送者 S 发送 *K*-匿名请求到其所在的簇的簇节点 AD1(若 S 为簇头节点的话则不用),然后由 AD1 形成一个随机偏移 $l$ 属于$[0,k-l]$。如果 S 所在簇中的车辆数小于 $k$,簇头节点 AD1 会向其前驱节点或者后继节点发出最小边界矩形的请求,如果仍未达到 $k$, AD1 将会反复这种请求操作,直到找到 $k$ 个车辆为止。簇头节点 AD1 收集到所有车辆的位置信息组合成 *K*- 匿名空间区域。对提出 *K*- 匿名请求的处理过程如下:

```
S. findASR( H, K)
  compute rank_H in sorted order of C_S
  generate random offset l
  begin = max(0, l - rank_H)
  end = max(0, k -1 + rank_H - size( C_S) )
  if( end > 0)
    succ. FwdReq( end, 1)
  if( begin > 0)
    pre. FwdReq( begin, 1)
wait for partial MBRs
K-ASR = union of all received MBR
S. K-request( K)
  call C_S. findASR( H( S), K)
S. FwdReq( count, direction)
  if( direction == 1)
    return MBR of first count keys
  if( count > size( C_S) )
    succ. FwdReq( count-size( C_S), 1)
  else
    return MBR of last count keys
      if( count > size( C_S) )
        pred. FwdReq( count-size( C_S), -1)
```

### 2.2.2 转发节点选择

定义 6 中将移动车辆间的连通性定义为车辆通信的最大距离与车辆间距离的比值,在不考虑障碍物的情况下,距离近的两个车辆间的连通性显然要比距离远的要好。只有车辆间处于通信范围之内才能建立匿名链路,即要求 $d$ 要小于 $R$,则 $St$ 小于 1。

假设有两个车辆起始位置距离为 $d$,分别以 $\boldsymbol{v}_1$、$\boldsymbol{v}_2$ 的速度运动,经 $t$ 时间后,记合速度向量与距离向量之间的夹角为 $\theta$,则有

$$|d'| = |d| + |\boldsymbol{v}|\, t\cos\theta \tag{1}$$

经 $t$ 时间后,以车辆间继续通信连通的概率来衡量车辆间的连通性,记为 $P(St \leqslant 1)$,则有

$$P(St \leqslant 1) = P\left(\frac{|d| + |\boldsymbol{v}|\, t\cos\theta}{R} \leqslant 1\right) = P\left(\frac{R - |d|}{t\cos\theta}\right) \tag{2}$$

一般车辆的速度值服从均值为 $\mu$、方差为 $\sigma$ 的正态分布,即 $|\boldsymbol{v}| \sim N(\mu,\sigma)$,则有

$$P(St \leqslant 1) = P\left(|\boldsymbol{v}| \leqslant \frac{R - |d|}{t\cos\theta}\right) = \frac{1}{\sigma\sqrt{2\pi}} \int_0^{\frac{R-|d|}{t\cos\theta}} \exp\left(-\frac{(|\boldsymbol{v}| - \mu)^2}{2\sigma^2}\right) \mathrm{d}|\boldsymbol{v}| \tag{3}$$

从式(3)可以看出,影响车辆间连通性是主要因素是距离 $d$、速度 $\boldsymbol{v}$、时间 $t$ 和速度与距离向量间的夹角 $\theta$。因此在选择转发节点时,*K*-匿名链机制根据车辆间的连通性来优化选择。

### 2.2.3 *K*-匿名链查询过程

以图 2 为例,当发送者节点 S 提出查询请求并要求 $k$ 为 4 时,首先会通知本簇的簇头节点 AD1,之后 AD1 通知簇中成员 Node1、Node2 和 S 共同构建 $k=4$ 的匿名集合,形成匿名空间;接下来 AD1 会在其后继簇中随机选择 $n$ 个簇,并向该 $n$ 个簇的簇头节点发送选择节点信息。如图 2 中以 AD2、AD3 为簇头节点的簇为被选择的后继簇。簇头节点 AD2、AD3 依据节点间的连通性分别从本簇中选择若干个簇成员作为转发节点,如图 2,发送者节点 S 会根据 AD2 返回的簇成员节点的信息计算其与簇成员节点间的连通性,从而可以选择 Node3 作为 S 的下一个转发节点。同样,Node3 会选择 Node4 作为转发节点,Node4 选择 Node6 作为转发节点。之后通过簇头节点将这些转发节点的信息发送给 AD1,AD1 再将这些节点信息发送给 S。S 通过得到的转发节点的地址信息以及公钥对其进行反向加密,由 S 确定构建匿名链的顺序,并且这个顺序只有 S 知道,之后 S 根据这个顺序对转发节点的构建匿名链。匿名链构建完成后,AD1 将 *K*-匿名空间及查询请求一并发送到匿名链上进行转发,最后由接收者 R 向 LBS 服务器发送请求。经处理过的查询请求由 LBS 服务器直接发送给 AD1,然后由 AD1 发送给 S,由 S 自己对查询结果进行求精。至此,整个 *K*-匿名链机制查询过程完成。

值得说明的,是簇中成员节点的身份信息由簇头节点来维护,并复制到所有的簇成员节点中,簇与簇之间通过簇头获知所有各个簇中成员节点的身份信息。为了加强系统的容错性,簇头节点由簇成员节点周期性地轮流承担负载,当簇头节点的负载达到一定的阈值就会引发簇头节点的选举,阈值由簇头节点发送或接收到的信息数量来测量。同样,操作的通信开销也是通过传播的信息量来测量[12],其数量级为 $O(\log N)$,其中 $N$ 为移动节点的总数目。

## 3 安全性分析

本文提出的 *K*-匿名链机制中的 *K*-匿名空间隐藏了发送者的真实位置,而匿名链则隐藏了车辆身份信息与位置信息的关联关系。因此,攻击者的目标是获取发送者的真实的位置信息及其匿名链隐藏的关联关系。

假设攻击者是一个全局攻击者,即攻击者可以获取 LBS 服务器数据,并且在移动节点内有同伙恶意节点。在一个包含 $n$ 个车辆及 $c$ 个恶意节点的网络中,为了简化讨论本文只考虑一种静态模型,即不考虑车辆的加入或者离开。在构造匿名链过程中,一些恶意节点可能被选为转发节点,这些恶意节点可以根据匿名链中转发节点的顺序以及匿名链所允许的最大长度 $K$ 值推测出攻击者想要的信息。下面分别从发送者节点和接收者节点角度来分析 *K*- 匿名链的安全性。

首先从发送者节点的角度来分析 *K*- 匿名链机制的安全性。假设匿名路径上的第 $j(j \leqslant K)$ 个节点是第一个恶意节点,则该节点会以一定的概率去推测自它开始的第 $i(i \leqslant j)$ 个节点是发送者节点。令 $\rho(i)$ 表示推测自恶意节点第 $i$ 个节点为发送者节点的概率,$\varphi(i)$ 为该节点确实为发送者节点的概率,如下:

$$\rho(i) = 1/j \tag{4}$$

$$\varphi(i) = \left(\frac{n-c}{n}\right)^{i-1}\frac{c}{n} \tag{5}$$

使用$P(H_j)$表示位于匿名链上的第$j$个节点的攻击者成功推测出发送者节点事件的概率,则该概率为:

$$P(H_j) = \frac{1}{k}\sum_{i=1}^{j}\varphi(i)\rho(i) = \frac{1}{k}\sum_{i=1}^{j}\frac{1}{j}\left(\frac{n-c}{n}\right)^{i-1}\frac{c}{n} \tag{6}$$

接下来,从接收者节点的角度来分析 $K$- 匿名链机制的安全性。假设最后一个恶意节点在匿名路径上的第$x(i \leqslant x \leqslant K)$个节点,则该节点会以一定的概率去推测自它开始的第$m(x \leqslant m \leqslant K)$个节点是接收者节点。令$\rho(m)$表示推测自恶意节点第$m$个节点是接收者节点,$\varphi(m)$表示该节点确实为接收者节点的概率,如下:

$$\rho(m) = \frac{1}{K-x} \tag{7}$$

$$\varphi(m) = \left(\frac{n-c}{n}\right)^{m-1}\frac{c}{n} \tag{8}$$

类似地,可以得出

$$P(H_m) = \sum_{i=x}^{K}\rho(m)\varphi(m) = \sum_{i=x}^{K}\frac{1}{K-x}\left(\frac{n-c}{n}\right)^{m-1}\frac{c}{n} \tag{9}$$

由以上分析可知,匿名链最大长度 $K$ 取值越大,相应的$j$与$x$的取值范围将增大,从而能够分别提高发送者节点及接收者节点的匿名程度,增加了恶意节点的攻击难度。从以上公式可看出,发送者节点的匿名程度明显高于接收者节点的匿名程度。这主要是由于发送者节点在发送查询请求前形成了 $K$-匿名空间,隐藏了发送者节点的真实位置。同样,恶意节点的数量会导致匿名程度的变化。当匿名链最大长度一定时,恶意节点数量增加会导致发送者节点和接收者节点的匿名程度下降;反之,它们的匿名程度会提高。

## 4　仿真实验与分析

为了验证 $K$-匿名链机制的有效性,在 Windows XP 操作系统环境下进行实验,利用 P2Psim 事件驱动型的数据包模拟器进行仿真。P2Psim 支持迭代和递归的路由查询,可以实现 Chord 分布式协议。实验使用德国 Oldenburg 实际的道路地图,包含 6 105 个节点和 7 035 条边。在实验中模拟不同交通状况条件下对连续位置的请求查询,移动节点的速度在 20 ~ 70 km/h。假设对请求连续位置查询用户每 10 s 发送一次服务请求。实验主要从 $K$-匿名链与匿名链匿名效果的比较、$k$的不同取值对 $K$-匿名链的影响以及采用转发节点选择优化与随机选择转发节点的比较三个方面进行了分析。

图 3 是在 1 000 个车辆的模拟环境,依次增加恶意节点的比例,$K$-匿名链与匿名链的长度都为 3 时且 $K$-匿名链的 $k$ = 3,分别计算它们中恶意节点成功推测出发送者节点的平均概率 $P$。图 3 中显示,当恶意节点比例增加时,本文提出的 $K$-匿名链与徐建等[8]的匿名链被成功推测出发送者节点的平均概率 $P$ 均增大,但 $K$-匿名链的 $P$ 值始终要低于匿名链的。说明 $K$-匿名链的匿名效果要好于匿名链。

如图 4 中所示,$K$-匿名链中匿名链的长度为 3,$k$ 取值从 10 到 100。随着 $k$ 值的不断增大,$K$-匿名链的匿名强度不断增加,攻击者能够鉴别发送者节点的概率不断下降。$K$-匿名链的匿名强度始终高于 $1/k$,说明 $K$-匿名链机制比单纯采用 $K$-匿名空间的匿名效果要好。如当 $k$ = 20 时,$K$-匿名链机制鉴别出发送者节点的概率是 4%,是理论的 $K$-匿名 5% 的 0.2 倍。

图 5 是对转发节点的随机选择方法和优化选择方法的比较实验结果进行了统计分析,其中 $K$- 匿名链机制中匿名链的长度为 3。如图 5 所示,随着环境中移动用户数目 $N$ 的增加,$K$-匿名链机制的稳定性($P$ 值) 逐步提高,尤其转发节点经优化选择后稳定性高于随机选择的稳定性,从而说明了转发节点优化选择是很有必要的。

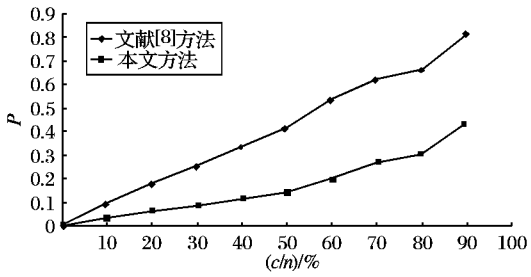

图 3　攻击成功概率

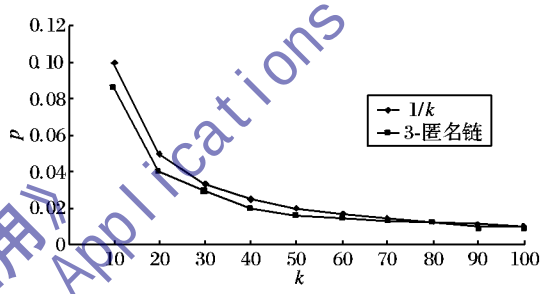

图 4　匿名空间 $k$ 不同取值对 $K$-匿名链的影响

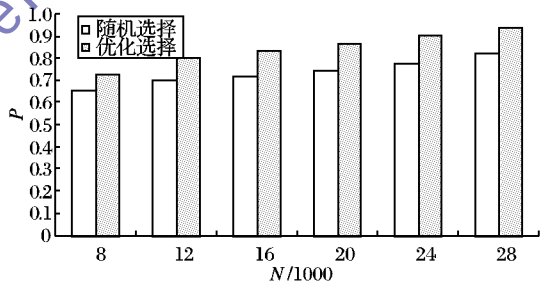

图 5　转发节点优化选择效果

## 5　结语

本文针对当前匿名链对移动车辆隐私性保护不足,提出了一种 $K$- 匿名链机制。对发送连续位置查询请求的车辆进行了 $K$- 匿名保护,并通过转发节点传递包含查询节点在内的 $K$-匿名空间及其查询请求构建匿名链。在保证查询节点 $K$- 匿名的条件下,隐藏了其身份信息与位置信息的关联关系,从而提高了车载网络中车辆的匿名强度。通过对仿真实验结果的分析,在同等条件下,$K$- 匿名链机制的匿名效果要明显好于匿名链的匿名效果,进一步完善了车载网络的安全性。

**参考文献:**

[1]　常促宇, 向勇, 史美林. 车载自组网的现状与发展[J]. 通信学报, 2007, 28(11): 116 - 126.

[2]　张新潮. 城市车载网络中的路由算法研究[D]. 上海: 上海交通大学, 2012.

[3]　RAYA M, AZIZ A, HUBAUX J P. Efficient secure aggregation in VANETs[C]// VANET 2006: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks. New York: ACM Press, 2006: 66 - 75.

(下转第 2524 页)

态链接库实现,使所有哨兵共享此部分代码,在被保护软件中仅植入跳转指令,这些跳转指令相对于整个软件来说所产生的空间开销是微不足道的,远低于前者的 50%。

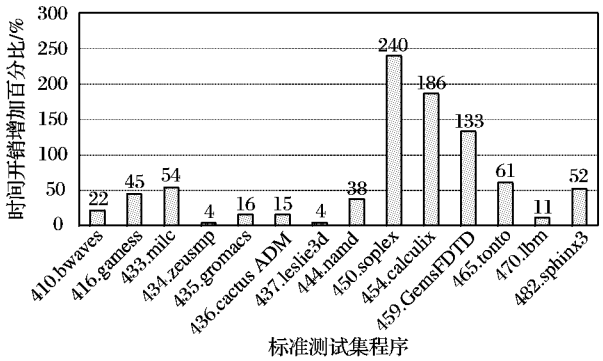


图 4 各基准测试程序植入哨兵后的运行时间

### 3.3 系统兼容性

该系统在进行哨兵植入时借助 Dyninst[15] 插桩框架和在其基础上实现的 Cobi[16] 可配置二进制插桩器实现。由于 Cobi 目前只能实现对 ELF 文件的分析操作,本系统目前只支持 Linux 操作系统。由于系统实现不需改变底层硬件和操作系统,该系统可在使用 Linux 操作系统的主机上快速移植、配置和应用。

## 4 结语

软件防篡改作为软件保护的一种重要手段,在软件保护领域具有重要作用和地位。为了防止控制流被篡改,本文提出一种基于函数级控制流监控的软件防篡改方法。方法为解决软件标准行为信息的存储问题,提出了信息树的标准行为描述方式,并借助 TPM 可信机制保证该信息的安全性。另外,方法通过采用植入哨兵并由哨兵发送软件运行状态报告的方式实现了软件行为信息的动态提取。最终在 Linux 系统上实现了一个原型系统,并验证了方法的有效性。下一步工作的重点是在现有方法的基础上,结合数据流分析和监控技术以提高对软件篡改的检测精度。

**参考文献:**

[1] ONE A. Smashing the stack for fun and profit[J]. Phrack, 1996, 7(49): 14 - 15.

[2] 王朝坤, 付军宁, 王建民, 等. 软件防篡改技术综述[J]. 计算机研究与发展, 2011, 48(6): 923 - 933.

[3] ABADI M, BUDIU M, ERLINGSSON U. Control - flow integrity principles, implementations, and applications[J]. ACM Transactions on Information and System Security, 2009, 13(1): 1 - 40.

[4] CASTRO M, COSTA M, HARRIS T. Securing software by enforcing data-flow integrity[C]// Proceedings of the 7th Symposium on Operating Systems Design and Implementation. Washington, DC: USENIX Association, 2006: 147 - 160.

[5] FORREST S. A sense of self for UNIX processes[C]// Proceedings of the 1996 IEEE Symposium Security and Privacy. Piscataway, NJ: IEEE Press, 1996: 120 - 128.

[6] HOFMEYR S A, FORREST S, SOMAYAJI A. Intrusion detection using sequences of system calls[J]. Journal of Computer Security, 1998, 6(3): 151 - 180.

[7] SEKAR R, BENDRE M, BOLLINENI P, *et al*. A fast automaton-based method for detecting anomalous program behaviors[C]// Proceedings of the 2001 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2001: 144 - 155.

[8] 李闻, 戴英侠, 连一峰, 等. 基于混杂模型的上下文相关主机入侵检测系统[J]. 软件学报, 2009, 20(1): 138 - 151.

[9] MAGGI F, MATTEUCCI M, ZANERO S. Detecting intrusions through system call sequence and argument analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(4): 381 - 395.

[10] 陶芬, 尹芷仪, 傅建明. 基于系统调用的软件行为模型[J]. 计算机科学, 2010, 37(4): 151 - 157.

[11] BLIETZ B, TYAGI A. Software tamper resistance through dynamic program monitoring[C]// SAFAVI-NAINI R, YUNG M. Digital Rights Management: Technologies, Issues, Challenges and Systems. Berlin: Springer, 2006: 146 - 163.

[12] KINDER J, VEITH H, ZULEGER F. An abstract interpretation-based framework for control flow reconstruction from binaries[C]// Proceedings of the 10th International Conference on Verification, Model Checking, and Abstract Interpretation. Berlin: Springer, 2009: 214 - 228.

[13] XU L, SUN F Q, SU Z D. Constructing precise control flow graphs from binaries[R]. Davis: University of Computer Science, 2009.

[14] PADMANABHUNI B, TAN H. Techniques for defending from buffer overflow vulnerability security exploits[J]. IEEE Internet Computing, 2011, 44(11): 53 - 60.

[15] BERNAT A R, MILLER B P. Anywhere, any-time binary instrumentation[C]// Proceedings of the 10th ACM SIGPLAN- SIGSOFT Workshop on Program Analysis for Software Tools. New York: ACM Press, 2011: 9 - 16.

[16] MUSSLER J, LORENZ D, WOLF F. Reducing the overhead of direct application instrumentation using prior static analysis[C]// Proceedings of the 17th International Conference on Parallel Processing. Berlin: Springer, 2011: 65 - 76.

(上接第 2519 页)

[4] KAMAT P, BALIGA A, TRAPPE W. An Identity-based security framework for VANETs[C]// Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks. New York, Press, 2006: 94 - 95.

[5] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J P, *et al*. Efficient and robust pseudonymous authentication in VANET[C]// Proceedings of the 4th International Workshop on Vehicular Ad Hoc Networks. New York: ACM Press, 2007: 19 - 28.

[6] KIDO H, YANAGISAWA Y, SATOH T. A anonymous communication technique using dummies for location-based services[C]// ICPS 2005: Proceedings of International Conference on Pervasive Services 2005. Piscataway, NJ: IEEE Press, 2005: 88 - 97.

[7] GHINTA G, KALNIS P, KHOSHGOZARAN A, *et al*. Private queries in location based services: anonymizers are not necessary[C]// Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. New York: ACM Press, 2008: 121 - 132.

[8] 徐建, 黄孝喜, 郭鸣. 动态 P2P 网络中基于匿名链的位置隐私保护[J]. 浙江大学学报: 工学版, 2012, 46(4): 712 - 718.

[9] 王岳. 稀疏车载网络路由算法的研究[D]. 桂林: 广西师范大学, 2012.

[10] 陈万顺. 基于 Chord 分布式哈希表的网络过载均衡方法[J]. 常州工学院学报, 2012, 25(6): 9 - 12.

[11] 路红. 物联网空间 LBS 隐私安全模型研究[D]. 武汉: 华中师范大学, 2012.

[12] 郭艳华. 位置服务中轨迹隐私保护方法的研究[D]. 武汉: 华中师范大学, 2011.