一种基于伪距离的VANETs的节点位置安全算法

徐会彬[1,2] 王 琦[3]
(同济大学电子与信息工程学院 上海 200092)[1] (上海师范大学天华学院 上海 201815)[2]
(上海财经大学人文学院 上海 200080)[3]

摘 要 由于VANETs的车辆的快速移动,基于地理位置的路由协议广泛应用于VANETs。车辆周期广播位置信息来建立路由,导致车辆的位置信息容易遭受泄露。为此,提出基于伪距离的位置隐私保护(false-based location privacy protection,FLPP)路由协议。在FLPP中,通过转发节点到目标节点的伪距离而不是真实距离来建立路由,通过巧妙地设置节点的定时器来保护节点的位置信息,同时采用别名策略隐藏身份信息。仿真结果表明,FLPP具有较高的数据传输率以及位置隐私保护力度。

关键词 伪距离,位置隐私,基于地理位置路由,VANETs
中图法分类号 TP393 **文献标识码** A

False Distance-based Location Security Algorithm for VANETs

XU Hui-bin[1,2] WANG Qi[3]
(School of Electronics and Information, Tongji University, Shanghai 200092, China)[1]
(Shanghai Normal University Tian-hua College, Shanghai 201815, China)[2]
(Economics Collage of Humanity, Shanghai University of Finance and Economics, Shanghai 200080, china)[3]

Abstract Geographic-based location routing protocols are widely used in VANETs since vehicles move fast. Vehicles periodically broadcast its current location information, which results in the event that location information is vulnerable to leak. Therefore, the FLPP (false-based location privacy protection) routing protocols were put forward in this paper. In FLPP, it makes use of the false distance between forwarding vehicles and destinations vehicles to build routing, not the real distance. In order to protect the vehicle location information, the timer of vehicle was cleverly set, and at the same time, the pseudonym strategy was used to hidden identity information. The simulation results show that the proposed FLPP has the high data delivery ratio and the position of privacy protection.

Keywords False distance, Location privacy, Geographic-based location routing protocol, VANETs

1 引言

车辆自组织网络(Vehicular Ad hoc Networks, VANETs)作为智能交通的重要组成部分,通过车间通信以及车辆与路边设施间通信,高效地实现事故预警、辅助驾驶、道路交通信息查询以及Internet接入服务等多种应用[1]。人们预期在不久的将来,随着VANETs的大量部署,它在事故预警、保障交通安全、交通管理、乘客娱乐以及为用户提供舒适、安全的驾驶环境等方面将会起着至关重要的作用,有望成为物联网的典型应用之一[2]。

与移动自组织网络(Mobile Ad hoc Networks, MANETs)不同,VANETs中节点的频繁移动导致网络拓扑高速变化,因此基于位置的路由协议在VANETs得到广泛的应用。典型的有基于地理位置的路由协议GPSR(greedy perimeter stateless routing)[3]、AODV[4]等。这些协议需要节点在一跳邻居内周期地发送beacons消息,实现节点位置信息的交互。这一过程就泄露了节点的位置信息以及身份信息,恶意节点[5]通过获取节点的位置信息进行跟踪等不轨的行为。例如,恶意节点通过偷听来自某节点周期的beacons消息,就能识别这个节点位置信息和身份信息。

节点的位置信息的泄露无疑阻碍VANETs广泛应用。目前,在基于地理位置的协议中,保护位置隐私有两种途径:1)直接隐藏节点的位置信息;2)保护用户的身份信息,使节点的位置信息与身份具有不可连接性。所谓的保护用户的位置隐私,就是指不向未认证的节点泄露车辆当前及过去的位置信息,未认证的节点可能是恶意的基础设施或行驶的车辆。

本文为保护节点的位置信息,采用基于竞争转发的通信模型[6],即不广播节点的位置信息。在基于竞争转发的方式中,仅参与路由的节点广播其位置信息,才能使其他节点的位置消息得以保护。为了更进一步保护参与路由节点的位置消息,本文提出基于伪距离的位置隐私保护协议(FLBB)。在FLBB中,数据包转发节点先向邻居广播其到目标节点的伪距离,基于这个伪距离,接收到此消息的邻居节点相互竞争,离目标节点最近的节点将成为下一跳节点。发送伪距离尽管使恶意节点不能获取转发节点真实位置信息,但是会影响基于地理位置的路由协议性能,因此伪距离的值需慎重地选取。

到稿日期:2012-07-29 返修日期:2012-10-03 本文受国家自然科学基金(60972036),上海市民办高校骨干教师科研项目资助。
徐会彬(1982—),男,博士生,讲师,主要研究方向为VANET安全技术、路由技术,E-mail:xuhuibin188@163.com。

在 FLPP 中，采用两道途径保护节点的位置隐私：第一，利用别名隐私节点的真实身份；第二，利用伪距离保护节点的位置信息。

2 相关研究

地理位置路由已广泛应用于 VANETs，实现了车与车之间、车与路边设施的通信[7,8]。与其他传统先应式路由[9,10]相比，基于位置信息的地理路由具有独特的优势。但是，在邻居节点间交互位置信息很容易导致位置信息的泄露。文献[11-13]均提出在 VANETs 中的位置隐私问题。

位置隐私保护可通过两种方式实现：第一种，隐藏数据发送节点的身份信息。在这种方式下，即使节点的位置信息被泄露了，恶意节点也无法将位置信息与身份相对应，从而更好保护了用户的位置信息[14,15]。这些方式大多数是通过周期地更换节点 ID。这种方案需要第三方的信任基础设施来维持运行。对于此方案来说，第三方的基础设施的投入以及节点与第三方的通信均增加了系统的负担，同时第三方本身也存在安全隐私问题。此外，频繁地更换别名极大地影响了路由性能，增大了数据包丢失率[16]。

第二种方法：数据包转发节点的真实位置隐私在某一区域内或在虚假数据的集合中[18]。例如：将节点的位置隐匿在一个三角或圆形区域内，在这个区域内至少有 $k-1$ 个其它的节点。这种方案也称为 k 匿名法，即恶意节点识别节点的真实身份的概率不大于 $1/k$。与 k 匿名法不同的是，文献[17]提出向邻居发送一些虚假数据，使接收节点无法从虚假数据中区分出真实的数据，从而保护用户的位置隐私信息。上述的这些方案，均是将节点的真实位置信息隐藏于一个区域或一个虚假数据的集合内，这将导致传统的路由协议在选择路由时无法获取正确的位置消息。

与上述不同的是，本文通过以下方式保护节点位置信息安全：1)在路由建立过程中，通过节点到目标节点的伪距离来替换节点的位置信息，即在建立路由时，不用节点的位置信息，而是用节点到目标节点的伪距离。2)通过别名保护用户的身份信息。通过这些改进，基于地理位置的路由协议仍然能继续工作，节点的身份和位置消息均得到保护。

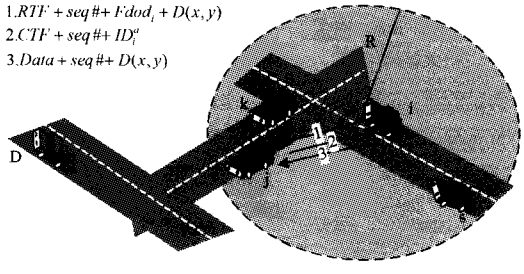

图 1 下一跳节点选择的信息交互过程示意图

3 算法描述

3.1 下一跳节点的选择

如图 1 所示，D 为目标节点，假设节点 i 收到一个数据包，其编号为 $seq\#$。节点 i 需要将 $seq\#$ 的数据包转发给目标节点 D，其目标节点为 $D(x,y)$。节点 j 是离目标节点最近的节点。节点 i 在转发数据包之前，先发送请求信息包 RTF，其格式为：

$$RTF+seq\#+Fdod_i+D(x,y)$$

式中，$Fdod_i$ 表示节点 i 到目标节点的伪距离。

邻居节点(假设为节点 a)收到 RTF 信息包后，首先确认此包是否在之前已接收过。如是之前已经接收过，则简单地丢弃此包，反之，节点 a 将 RTF 信息包存于缓冲区里，并设置定时器，定时器的运行时间为：

$$t(r_a)=f(1-1/r_a) \tag{1}$$

式中，r_a 为节点 a 到目标节点的距离，根据 RTF 信息包中的 $D(x,y)$ 计算 r_a。

由式(1)可知，每个节点的定时器的运行时间正比于其到目标节点的距离。离目标节点最近节点的定时器的运行时间首先计时完毕。如图 1 所示，节点 j 的定时器最先计时完毕，完毕后立即发送 CTF 信息包，CTF 信息包内容如下：

$$CTF+seq\#+ID_i^a$$

式中，ID_i^a 表示节点 a 的别名，这个别名是从别名库 l 中随机选择的。别名库采取预下载制，每个节点系统认证时下载一个别名库。在不同的 CTF 信息包中，节点的别名是不同的，即使是来自同一个节点的 CTF 信息包。

当其他的邻居节点收到来自节点 a 的 CTF 信息包时，立即取消自己的定时器，并停止发送 CTF 信息包的工作。由于只有在节点 a 的通信范围内的节点，即节点 a 的邻居节点才能收到来自节点 a 的 CTF 信息包，没有收到 CTF 信息包的节点有可能再次发送 CTF 消息包，因此节点 i 可能收到来自不同节点的 CTF 信息包。针对同一个 RTF 信息包，节点 i 第二次以及第二次以上收到不同节点的 CTF 信息包，本文将这些节点所在的区域称为冗余区域。

节点 i 第一次收到此 CTF 信息包，立即发送一个数据包 Data，此数据包用 CTF 信息包中的节点的别名加密。如果节点 i 正在发送数据包时，收到第二 CTF 信息包，节点 i 则简单地丢弃此 CTF 信息包。数据包 Data 的内容如下：

$$Data+seq\#+D(x,y)$$

节点 i 的邻居节点收到数据包 Data 时，如果之前没有发送过 CTF 信息包的节点，则不接收此数据包。反之，就用自己的在发送 CTF 时所用的别名去解密。通过 RTF 和 CTF 信息包的交互，节点 i 成功选取了下一跳的转发节点 j，并传递了数据包。

3.2 位置隐私保护

由 3.1 节所述可知，节点 i 可能收到多个 CTF 信息包，这将影响网络的性能，增加网络的负担。另外，恶意节点通过邻居节点的定时器的计时完毕时间，比较容易地获知它们到目标节点的距离，无意中向恶意节点暴露节点的隐私。因此，如何设置每个接收节点定时器的运行时间，以控制 CTF 信息包的发送数量是下文研究的重点。

从式(1)可知，任意一个节点的定时器的运行时间完全取决于由节点到目标节点的距离，因此，式(1)可修改为：

$$t(r)=T(1-1/r) \tag{2}$$

式中，T 为一跳转发的最大时延。

冗余响应的区域可由图 2 所示[18]。图中的斜线区域为冗余区域。假设有到目标节点的距离为 r_1 的节点，以及到目标节点距离为 r 的节点，如果这两个节点的定时器的运行时间很小，设：$t(r)-t(r_1)<\delta$，δ 为接收节点能区分的最小时间间隔，这两个节点之间就形成冗余区域。这个区域越大，重复发送 CTF 消息的节点就越多。

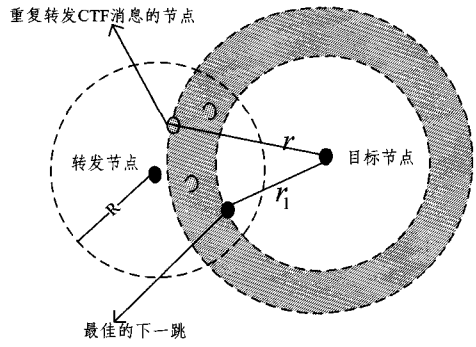

图 2　冗余响应示意图

根据式(2)，最适应的下一跳候选节点的定时器的运行时间为 $t(r_1)$，冗余节点的定时器的运行时间为 $t(r)$，则 $t(r)$ 满足以下的条件：

$$t(r_1)<t(r)<t(r_1)+\delta \tag{3}$$

因此，为了尽可能缩小冗余区域，应增大 $t(r)$，使接收节点有足够的区分时间。设

$$t(r)=T(1-\frac{1}{r_1})+\delta$$

$$=T\left(1-\frac{1}{r_1 T(T-\delta r_1)^{-1}}\right) \tag{4}$$

冗余区域宽度为：

$$r_1 T(T-\delta r_1)^{-1}-r_1=\frac{\delta {r_1}^2}{T-\delta r_1} \tag{5}$$

δ 是一个常数，因此，可设 $T=n\delta$。假设可接收的冗余区域的宽度为 Δ。

$$\frac{\delta r_1^2}{T-\delta r_1}=\frac{\delta r_1^2}{n\delta-\delta r_1}=\frac{r_1^2}{n-r_1}<\Delta \tag{6}$$

式(6)可知，T 的下限值为

$$T=\frac{r_1^2+r_1^2\Delta}{\Delta}\delta \tag{7}$$

从式(7)可知，节点到目标节点的距离越大，T 越值就越大。然而，在系统中，T 值应足够小，以缩短通信时延。为了解决这个问题，对式(2)进行修改。假设某一节点发送了 RTF 数据包，所有的接收节点均按照式(8)而不是式(2)设置定时器的运行时间。

$$t(r)=T\left(\frac{r-\bar{r}_f}{3R}\right) \tag{8}$$

式中，R 表示节点的通信范围，r 是表示收到 RTF 的接收节点到目标节点的距离，$\bar{r}_f$ 表示发送 RTF 信息包的节点到目标节点的伪距离[18]，$\bar{r}_f=Fdod$。由于 $\bar{r}_f$ 是随机的，发送 RTF 信息包的节点以及接收 RTF 信息包的节点的位置应隐私保护。

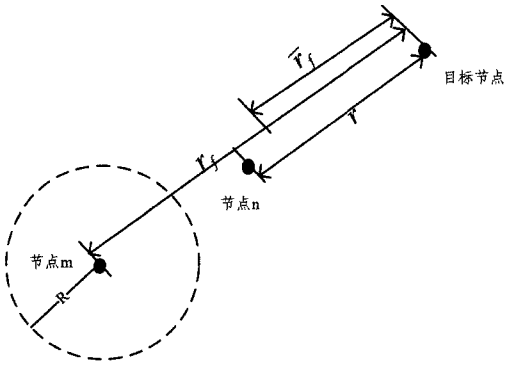

图 3　转发节点中的伪距离选择示意图

如图 3 所示，假设节点 m 发送了 RTF 的信息包，其到目标节点的真实距离为 r_f，$\bar{r}_f$ 表示节点 m 到目标节点的伪距离。节点 n 收到 RTF 信息包，并设置定时器，节点 n 到目标节点的距离为 r，则节点 n 的定时器的运行时间 $t(r)$ 按式(8)计算。

$$\bar{r}_f=r_f-(1+\rho)R,\rho\in[0,1] \tag{9}$$

从式(9)可知，节点 m 的真实位置隐藏于半径为 R 的区域内，其到目标节点的真实距离与伪距离的差值，即 $(r_f-\bar{r}_f)\in[R,2R]$，节点 m 的真实位置得以保护。

由于节点 m,n 属于邻居节点，$r-r_f$ 的值在 $[-R,R]$ 范围内，因此，

$$r-\bar{r}_f=r-r_f+(1+\rho)R\in[0,3R]$$

由于，$0<r-\bar{r}_f<3R$，可知 $\frac{(r-\bar{r}_f)}{3R}<1$，推导出 $t(r)$ 小于 T，即节点 n 的定时器的运行时间在 $[0,T]$ 范围内，不会超越一跳最大时延。

接下来，推导冗余区域的宽度：

$$t(r)-t(r_1)<\delta\Rightarrow T(\frac{r-\bar{r}_f}{3R})-T(\frac{r_1-\bar{r}_f}{3R})<\delta$$

$$\Rightarrow r-r_1<\frac{3R}{T}\delta$$

假设，可接受的冗余区域的宽度为 Δ，则

$$\Delta=\frac{3R}{T}\delta\Rightarrow T=\frac{3R}{\Delta}\delta \tag{10}$$

与式(7)相比，式(10)的 T 减小了很多，当 R,Δ,δ 一定时，T 值固定，其在 VANETs 中可接受。

4　仿真结果分析

4.1　算法的性能指标

为了更好地描述算法的性能，本文分别从数据传输速率(Data delivery ratio，DDR)、端到端的传输时延(End to end delay，ETED)、位置隐私保护能力 3 项数据分析本文所提出的算法。DDR 为目标节点所接收的数据包与源节点所发送的数据包的比值。ETED 表示网络从源节点到目标节点传输数据包的平均时间。用隐私熵来描述针对位置隐私保护的性能。在信息理论中，熵用于量化评价不确定的系统。在本文仿真中，用隐私熵表示算法的保护隐私能力。隐私熵的值越大，隐私性能越好。隐私平均熵(Privacy Average Entropy，PAE)为一个恶意者去获取节点的位置和身份信息所要求的平均熵。

4.2　仿真环境及模型

本次仿真选取了一个较为简单的场景，如图 4 所示。在一个 4 车道、每车道宽 2.5m、长 1000m 的高速公路上，180 车辆随机分布。车辆的行驶速度为从 15～35m/s 随机选取。每节车辆的通信范围为 250m。采用 ns_2.29 软件对 FBLPP 进行仿真，并将 GPSR、CBF-AS、GPSR-ID 3 个协议和本文所提出的 FBLPP 算法分别从 DDR、ETED、PAE 方面进行比较分析。

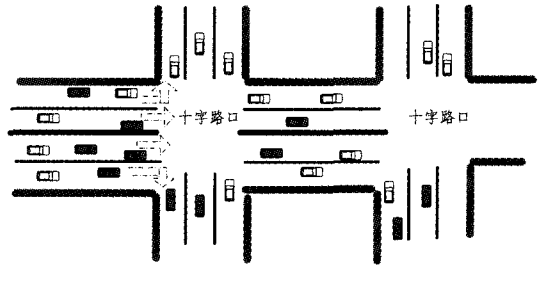

图 4　仿真中的车辆模型

4.3 仿真结果分析

如图5所示，FBLPP、CBF-AS-ID和GPSR具有类似的数据传输速度速率。GPSR-IR数据传输速率最低，主要是由于下一跳的转发节点需频繁地更换它的ID。在GPSR协议中，通过从beacon消息中获取邻居节点的信息建立下一跳节点。由于邻居节点的位置信息变化较快，邻居列表中可能存在已过时邻居。这将使数据包无法成功传递，导致数据传输速率略低于FBLPP、CBF-AS-ID。然而，在FBLPP协议中，通过相互竞争方式选择下一跳节点，赢者将成为下一跳节点，数据包传递给已过时的邻居的几率比GPSR低。

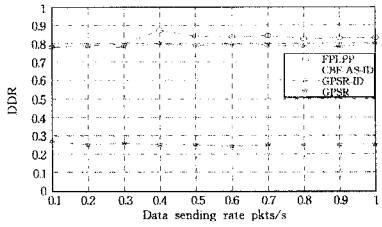

图5 DDR随数据发送速率的变化图

如图6所示，与FLBPP、CBF-AS-ID相比，GPSR和GPSR_ID具有比较小的时延。这主要是因为，在FLBPP、CBF-AS-ID协议中，节点发送了一个RTF信息包，邻居节点需要启动定时器，这一过程导致了额外的时延。尽管FLBPP与CBF-AS-ID均属基于竞争机制，但FLBPP具有更高的EED，这主要是由于冗余区域导致信息重复地交互，使得网络拥塞从而增加EED，其可通过减少 T 来降低EED。

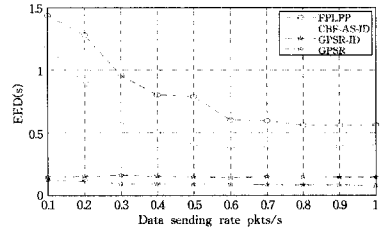

图6 EED随数据发送速率的变化图

如图7所示，在FBLPP中，为了使攻击节点的位置隐私，恶意节点需要更多的比特信息。在GPSR，每个节点周期地广播beacons，beacons包含节点的位置信息，因此，恶意节点获取车辆的位置信息的熵近为0。CBF-AS-ID和GPSR-ID尽管有一定的保护隐私的能力，但不如FPLBB，这主要是由于FPLBB不但采用别名机制，而且发送的是伪距离，这为恶意节点攻击其它节点的位置信息增加了难度。

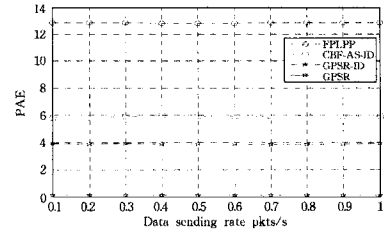

图7 PAE随数据发送速率的变化图

结束语 针对地理位置路由协议中的位置信息泄露，提出了基于伪距离的位置信息隐私保护机制。在提出的FBLPP中，节点无需交互它们的位置信息，只需交互它们到目标节点的伪距离。同时，采用别名机制，隐藏节点的身份信息。仿真结果表明，FLBPP具有很高的位置信息保护能力。当然，本文提出的算法有待优化。今后，将关注VANETs的位置信息隐私保护算法，同时改进本文提出的算法，使算法适应于更复杂的环境并提高算法的性能。

参 考 文 献

[1] Willke T L, Tientrakool P, Maxemchuk N F. A Survvey of intervehicle communication protocols and their applications [J]. IEEE Communications Surveys & Trtorials, 2009, 11(2): 3-20

[2] Lee J H, Chilmakurti N. Performance Analysis of PMIPv6 based Network Mobility for Intelligent Transportation Systems[J]. IEEE Transaction on Vehicular Technology, 2011: 23-32

[3] Karp B, Kung H T. GPSR: Greedy perimeter stateless routing for wireless networks[C]// Proc of 6th Annual International Conference on Mobile Computing and Networking. 2000: 243-254

[4] 宋利民，董贤伟，何荣希. 基于位置信息的改进AODV路由算法[J]. 计算机工程与设计，2012，33(2)：455-461

[5] Chang Shan, Qi Yong, Zhu Hong-zi, et al. Footprint: Detecting Sybil Attacks in Urban Vehicular Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011: 1-13

[6] Fler H, Widmer J, Ksemann M, et al. Contention-based forwarding for mobile ad hoc networks[J]. Ad hoc Networks, 2003, 1(4): 351-369

[7] Zhao J, Cao G. VADD: Vehicle-assisted data delivery in vehicular ad hoc networks[C]// IEEE international Conference on Computer Communications. 2006: 1-12

[8] Yang Q, Lim A, Agrawal P. Connectivity aware routing in vehicular networks[C]// Wireless Communications and Networking Conference. 2008: 2218-2223

[9] Naumov V, Gross T. Connectivity-aware routing (CAR) in vehicular ad-hoc networks[C]// Proceedings of the 26th IEEE International Conference on Computer Communications. 2007: 1919-1927

[10] Lee K, Le M, Haerri J, et al. Louvre: Landmark overlays for Urban Vehicular routing environments[C]// Proceedings of IEEE Vehicular Technology Conference. 2008: 1-5

[11] Hao Jiang-guo, Dai Yi-qi. Achieving Controllable Privacy Protection in Position Service for VANETs[J]. Chinese Journal of Electronics, 2011, 20(3): 395-401

[12] Lu Rong-xing, Lin Xiao-dong, Liang Xiao-hui. A Dynamic privacy-preserving key management scheme for location-based services in VANETs[J]. Intelligent Transprotation System, IEEE Transactions on, 2012, 13(1): 127-140

[13] Lu R, Lin X, Zhu H, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[C]// The 27th Conference on Computer Communications. 2008: 1229-1237

[14] Sampigethaya K, Huang L, Li M, et al. Providing location privacy for VANET[C]// Proceedings of Embedded Security in Cars. 2005

[15] Freudiger J, Raya M, Flegyhzi M, et al. Mix-Zones for location Privacy in Vehicular Networks[C]// Workshop on Wireless Networking for Intelligent Transportation Systems. 2007

[16] Schoch E, Kargl F, Leinmuller T, et al. Impact of Pseudonym Changes on Geographic routing in VANETs[C]// European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2006). 2006: 43-57

[17] Kido H, Yanagisawa T Y. Satoh. Protection of location privacy using dummies for location-based services[C]// 21st International Conference on. 2005: 1248-1248

[18] Qing Y, Alvin L. Location privacy protection in contention based forwarding for VANETs[C]// IEEE Global Telecommunications Conference. 2010: 1-5