DOI:10.13878/j.cnki.jnuist.2017.05.004

赵佳[1,2]　李娜[1,2]　韩磊[3]　刘吉强[1,2]

城市环境下基于车辆分类的车载自组网隐私保护方案研究

摘要

车载自组织网络的出现,在提高交通效率、改善交通环境的同时,也带来例如消息篡改、伪造和身份信息泄露等安全威胁.这就要求设计出更加符合车载网特性的消息认证方案.本文提出一种城市环境下的车载自组织网络隐私保护方案,其中包括对车辆进行分类,以及为不同类别的车辆分配不同的信任值的方法.在私人车辆认证的过程中采取一种假名多次签名方案对消息进行签名,在公用车辆和固定单元不需要身份隐私保护的情况下可以直接选用RSA签名方案对消息签名,在签名的同时都需要使用对信任值进行累加的策略来提高消息的可靠性.最后使用SUMO、MOVE和NS2进行联合仿真实验,结果表明该方案具有较好的灵活性,而且认证时间小于其他方案.

关键词

车辆分类;隐私保护;信任度量;假名

中图分类号 TP309.2

文献标志码 A

收稿日期 2017-05-31

资助项目 国家自然科学基金青年科学基金(61502030);中央高校基本科研业务费(2016JBM020)

作者简介

赵佳,女,副教授,主要研究车载网隐私保护、数据安全、可信计算等.zhaojia@bjtu.edu.cn

1 北京交通大学 智能交通数据安全与隐私保护技术北京市重点实验室,北京,100044

2 北京交通大学 计算机与信息技术学院,北京,100044

3 中国人民解放军66019部队,北京,102212

0 引言

据世界卫生组织报告显示,近年来由交通事故造成的死亡人数逐年增多(占事故总死亡人数的比例接近3.4%).世界范围内道路交通事故每年约夺取130万人的生命,道路交通事故已经成为全球公共安全的杀手.2003年国际电信联合会的车辆通信规范化会议上,已将车载自组织网络(Vehicular Ad Hoc Network,VANET)概念化.车载自组织网络的出现有利于车辆之间的“交流”,成为智能交通系统的重要基础,是对传统的自组织网络的功能扩展,使得驾驶员不只是依靠眼睛观察车辆状况(车速、转向、紧急停车等)和道路顺畅程度信息.车载自组网的推行将最大限度地减少或避免交通事故,提高旅途通行效率,为驾驶员和乘客的旅途带来安全和舒适.

近年来,世界各国政府、研究机构和学术界都对VANET的研究产生了兴趣.IEEE在无线网络通信协议的基础上提出了可以被用在车载通信(或称专用短距离通信,Dedicated Short Range Communications,DSRC)体系中的车间无线通信接入框架(Wireless Access in Vehicular Environments,WAVE).美国联邦通信委员会(Federal Communication Commission,FCC)专门为车间通信划分出了75 MHz的专用频段.如图1所示,为每个频段分配10 MHz的带宽,DSRC的通信频段共分为7段.其中,道路事故避免和其他耗能高的应用处在边缘位置;控制频段在Ch178,确保车辆通信安全,剩下4个频段可以用在安全或者非安全的情况下.

在车载自组织网络中,通信方法有两类:

1)驾驶的车辆之间(Vehicle to Vehicle,V2V);

2)驾驶的车辆与固定单元之间(Vehicle to Roadside Unit,V2R).

为了保证消息的可信任性、完整性、来源可认证性,需要对消息进行签名,但是私家车辆和执行任务的公用车辆不希望暴露自己的身份,因此在研究中通常采取假名签名方案.

文献[1-3]针对车载网的安全问题进行了研究,文献[4-6]讨论了影响用户安全的因素.主要包括4个属性维度的攻击[7]:

1)内部攻击和外部攻击:内部攻击主要是对经过车辆管理中心授权的合法车辆的攻击;外部攻击指的是没有被车辆管理中心授权

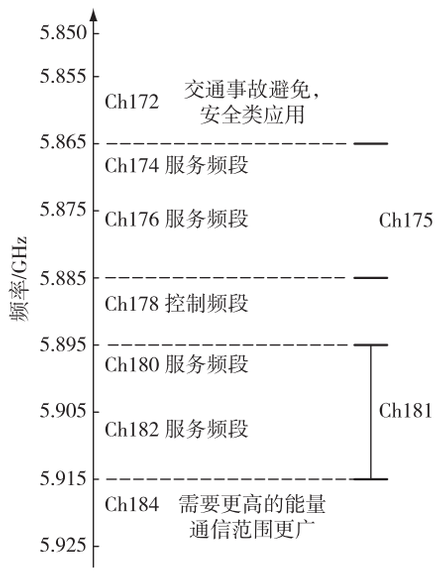

图 1 车载自组织网络中的频段划分

Fig. 1 Channel division of VANET

的车辆,非法进入网络的内部.

2)恶意攻击或者理性攻击:前者不是为了个人利益,仅仅为了破坏网络的正常通信;后者则是为了个人的好处而进行的攻击.

3)主动攻击或者被动攻击:前者对消息进行捏造和更改;后者只能对消息进行窃听.

4)局部攻击和全域攻击:前者指的是在某一个特定的范围内进行攻击;后者则是对全部通信范围进行的攻击.

为了防止以上的攻击对车辆产生威胁,结合车载网中的车辆移动的速度比较快的特点,就要求设计出的方案更加安全高效.假设一条道路上,既有私人车辆又有公用车辆,私人车辆发出一条关于道路状况的信息,由于私人车辆发出信息的可信度很低,因此其他车辆不会信任它发出的信息,需要与自身发出的信息进行对比,再将信息进行签名后发送出去,然而同样一辆行驶在道路上的警车,发出一条道路状况信息,这条信息的可信度对比于其他私人车辆发出的信息的可信度会更高.当周围的车辆收到这种警车发出的信息时,就可以直接进行接收.那么在消息的接收过程中怎样来快速区分是哪一种车辆发出的信息,如何更好地利用公用车辆的这一优势,使得消息的认证过程更加高效,成为目前的研究热点.

本文中,采取了为不同类型的车辆设置不同的信任值的方式,在消息被签名的同时,为了防止车辆的合谋攻击,需要对相应车辆的信任值进行累加,当信任值达到某一阈值时,则认为该消息是可靠的,这样就不仅可以提高消息传递的效率,也保证了消息的可靠性,进而防止交通事故的发生.

1 相关工作

1.1 研究现状

文献[8]中提出了一种方案,在该方案中固定单元(可认证 RSU)可以快速地认证车辆匿名发送的安全消息并广播给车辆,使消息的认证效率大幅提升.为了进一步提高消息的认证效率,它又对该方案进行了改进,采用信任值累加的方式,不同的车辆对相同消息的签名会产生信任值的累加,当信任值达到阈值时就认为消息是可靠的,这样很好地抵挡了合谋攻击.文献[9]提出了车辆分类认证的思想,根据是否需要保护隐私把车载自组网的通信实体分为两类,需要保护隐私的车辆采用群签名的方案,不需要保护隐私的车辆以及固定单元(RSU)采用基于身份的认证机制.虽然该方案可以节约运算时间,但是这两种签名机制是完全分离的,不能很好地适应不同环境下的应用问题.例如,在某些情形下,警车可能对身份信息保护也有需要.文献[10]用代理签名的方案来解决移动中的车辆节点的认证问题,节点对同一个信息的重复认证问题由代理多次签名来解决,在车载节点之间创立基于盲签名认证技术的交互性,适用于复杂的车载通信系统.本文也借鉴了文献[10]的优点,将每一次的签名信息都保留,防止对同一条消息进行多次的重复签名.

文献[11]提出了一种不需要证书的匿名认证方案,该协议省略了证书管理及密钥托管过程.在此方案中,满足了消息的不可否认性、相互认证性、条件隐私保护性、抗重放攻击等性质.但是该方案在消息认证的过程中需要频繁地与 DMV 进行交互,来获得 OBU 的私钥.文献[12]开发出了一个有效的隐私保护协议(Efficient Conditional Privacy Preservation, ECPP),这是第一个支持合法车辆通过 RSA 快速更新短时匿名证书的协议,但是要求道路上很短的距离就要放置一个 RSU,车辆携带的假名证书的生存时间是很短的,所以对于车辆来说存放消息撤销列表的副本是没有必要的.该方案虽然提高了效率,但是对 RSU 的分布距离要求比较高.

近几年,对将匿名技术用于群签名中也进行了大量的研究.文献[1]为了避免在批量验证的过程中

如果遇到一条非法签名就要丢弃整批签名的缺点,设计出了二分查找算法,并且在群签名的过程中引入了布鲁姆过滤器,提出了 SPECS 算法.文献[13]则提出了一种群签名批量消息认证方案,但是该方案计算难度比较大,车辆召回和密钥更新都要付出很大的时间代价.

以上方案大多采用了比较传统的群签名或者是匿名签名机制.本文结合以上研究中的长处,充分利用不同车辆的特性差别对车辆分类管理,来区分车辆的隐私保护需求,也为不同的车辆分配了不同的信任值,充分利用那些可信赖的特种车辆,来缩短整个车载网络的认证时间.通过对消息的重复签名,以及对消息签名信息的保留,防止同一个消息被相同的发出者重复签名,也提高了消息伪造的难度.

1.2 RSA 消息签名算法

RSA 也可以用来为消息签名[14].如果 Alice 想给 Bob 发送一个签过名的消息,那么 Alice 可以算出消息的散列值,再用 Alice 的私钥加密这个散列值,最后将散列值附带在消息的后面.这个消息只有用 Alice 的公钥才能解密,Bob 在收到这个消息后可以用 Alice 的公钥解密这个散列值,然后用这个数据与 Bob 自己为这个消息计算的散列值进行对照.如果两者完全相同,那么他就可以知道发信人确实是 Alice,并且可以确定这个消息在传播过程中没有被篡改过.

获得散列值的方法是使用哈希函数.哈希函数把消息或者数据进行压缩变成摘要,使得数据长度变短,并产生固定格式的数据.

哈希函数具有以下两个性质:

1)确定性:如果同一个哈希函数所得出的散列值不同,那么两个散列值的原始输入也不同.

2)单向性:给定散列后的消息值,很难计算出散列前的消息.

1.3 系统模型

VANET 的系统模型主要包括 3 部分[15].如图 2 所示,通信实体由车辆管理中心(Department of Motor Vehicle,DMV)、车载通信单元(OBU)以及固定单元(RSU)3 部分组成.OBU 和 OBU、RSU 和 OBU 之间采用的通信方式是无线通信,DMV 和 RSU 之间采用的通信方式是有线通信.

1)车辆:是车载自组织网络中最不可缺少的组成部分,车辆中都安装有无线通信模块 OBU,在车载自组织网络中车辆能够接收和发送信息.

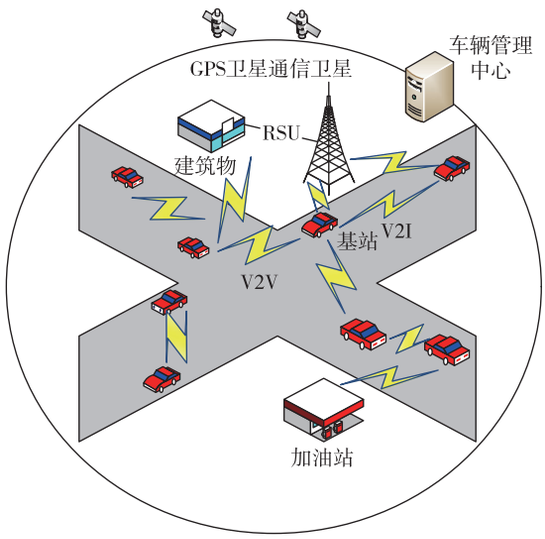

图 2 车载自组织网的系统模型

Fig. 2 System model of VANET

2)DMV:是负责车辆和 RSU 注册的可信任中心.DMV 在车辆和 RSU 进行注册的时候,会保留车辆和 RSU 的账户列表,可以为车辆和 RSU 发放签名证书和公私密钥对.

3)RSU:RSU 类似于车辆,装配了无线通信设备,可以进行数据的处理和分析.RSU 在道路上的分布不是均匀的,要根据具体的交通状况来确定,在车辆比较密集的地方,RSU 的分布相对来说较为密集.RSU 可以作为消息的中转站,将 DMV 和车辆连接起来.

在车载网中,每一辆车都安装了能够精确定位和获得时间信息的 GPS 定位系统和可信平台模块(Trusted Platform Module,TPM),它能有效地保护数据,防止非法用户访问.为了数据的安全考虑,车载单元(OBU)中都集成了安全芯片,可实现数据加密、密码保护等安全功能.RSU 是一种安装在路边的固定通信单元,RSU 可以从车辆管理中心获得 OBU 的账户列表,与合法的 OBU 进行通信.

2 车载网中基于信任值的重复签名协议

本文提出了一种基于车辆信任值的重复签名算法.在该算法中,要为不同的车辆赋予不同的信任值.另外,为了防止私人车辆的身份泄露,采取匿名签名与信任值相结合的方式进行消息的认证.车辆所使用的假名、假名的证书、不同车辆的信任值是由车辆管理中心(DMV)在车辆注册的时候统一存储在车辆的防篡改元件 TPM 中的.对于不需要保护隐私的

公用车辆直接用公用车辆的真实身份进行签名.该方案可以更好地适应不同车辆在不同场合下的安全需求,打破了传统方案中单一的签名方式缺乏灵活性的缺点.

1)系统初始化

①初始化:由 DMV 来执行,生成系统参数.本文的 RSA 加密算法,选择的密钥长度是比较主流的 512 bit,将要用到的参数如表 1 所示.首先为 DMV 选取两个大素数 p_{DMV} 和 q_{DMV},其中 $N=p_{\mathrm{DMV}}q_{\mathrm{DMV}}$,计算欧拉函数 $\emptyset(N)=(p_{\mathrm{DMV}}-1)(q_{\mathrm{DMV}}-1)$,随机选择一个数 e $(1<e<\emptyset(N))$ 与 $\emptyset(N)$ 互质,计算 $d=\mathrm{e}^{-1}\bmod \emptyset(N)$,经过计算产生出 DMV 的公私密钥对分别为 $PK_{\mathrm{DMV}}(e,N)$ 和 $SK_{\mathrm{DMV}}(d,p_{\mathrm{DMV}},q_{\mathrm{DMV}})$.DMV 还要选取一个安全的单向哈希函数 $H:\{0,1\}^{*}\rightarrow Z_N^{*}$ 在签名以及后面的消息验证过程中使用.

表 1　符号变量列表

Table 1　Symbolic variables and correspondent meanings

符号	表示的意义
SK_X	X 的私有密钥
PK_X	X 的公共密钥
Cer_{IDX}	不同 IDX 的证书
Sec	车辆的信任值
$SThre$	消息的安全阈值

②注册:车辆和固定单元都需要向 DMV 进行注册,在对 RSU 进行注册时 DMV 为 RSU 分配公私密钥对 SK_{RSU}、PK_{RSU}、证书 Cer_{RSU} 以及信任值 Sec.对车辆进行注册时,要为车辆分配它们的 ID 号、假名,以及基于假名和真实 ID 的证书 Cer_{IDX} 和信任值 Sec.在本文中,为不同的车辆设定的信任值分别是:警车和 RSU 的信任值=30、公共汽车的信任值=25、出租车的信任值=20、其他私人车辆的信任值=15.并且设定消息的安全阈值=35.在消息的传输过程中,经过信任值的累加达到这个安全阈值,就认为该消息是可靠的.由于本文中的 RSA 加密算法所选择的密钥长度为 512 bit,所以 RSA 每次加密的消息不能超过 512 bit.本文对消息的数据结构进行了具体的设计,如图 3 所示,车辆在 DMV 注册后生成的信息中包括车辆的信任值、车辆的真实 ID 或基于假名的 ID、第一个签名者发送消息的时间(在后文中简称发送时间)、生存时间、数据信息(路况)以及消息的签名信息.车辆的信任值、车辆的假名以及假名的证书和哈希函数都将存储在车辆的防篡改元件 TPM 中.

2)消息的签名和认证

①签名的过程:当车辆或者 RSU 发出自己周边道路环境状况的信息(道路的拥堵状况、是否有交通事故发生、道路的平均车速等)时,本文中设定大部分信息都是由 RSU 签名后发出的.假定 RSU 发出的消息为 $m\in Z_N^{*}$,当 RSU 生成消息 m 时就将自己的公钥证书嵌入到了签名信息字段中,消息的接收者可以利用这个签名证书对消息进行认证.首先计算消息 m 的哈希值 $H(m)$,然后用 DMV 分配给 RSU 的私钥进行签名,则 $H(m)$ 的签名为

$$Sig(H(m))=H(m)^{d_{\mathrm{RSU}}}\bmod N_{\mathrm{RSU}},$$

RSU 将签名信息计算完后,就将 $Sig(H(m))$(后面用 $S_i(i=1,2,\cdots,n)$ 表示)嵌入到消息 m 的后面,作为消息的摘要信息,然后将消息发送出去.

②签名的验证过程:其他车辆在收到 RSU 发出的信息时,首先要对消息的生存时间和信任值进行检查,如果消息的信任值 Sec 没有达到消息的安全阈值 $SThre$,那么车辆会将收到的数据信息和自己要发出的数据信息做对比,仅对比该路段是否有交通事故和道路是否拥堵两方面的信息,如果和自身信息相符,就进行下一步骤,即对 RSU 发出的消息用它的假名证书或者真实 ID 证书进行签名信息的验证,当 RSU 收到 m 和 S_1 后,计算:

$$H(m)'=S_1^{e_{\mathrm{RSU}}}\bmod N_{\mathrm{RSU}},$$

如果 $H(m)=H(m)'$,则消息确实是由 RSU 发送过来的并且没有被篡改过.签名以及签名验证的详细过程如图 4 所示.

③消息信任值的累加:在确认了消息的完整性和来源之后,就要对消息的信任值进行累加,当前信任值=收到消息的信任值+车辆自身信任值 Sec,将累加的结果写入到相应的数据字段.

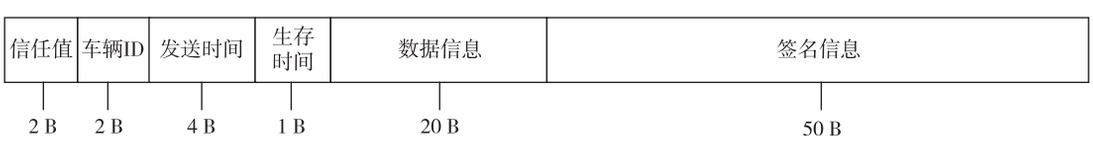

图 3　车辆信息格式

Fig. 3　Vehicle information format

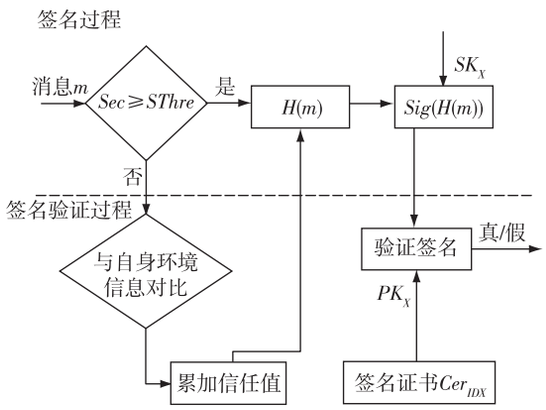

图 4　数字签名及验证过程

Fig. 4　Process of digital signature and verification

完成消息的认证和信任值的累加之后,车辆 V_{IDX} 将自己的签名证书附加到签名信息字段,然后对修改了信任值的信息 m 进行签名,将消息的摘要 S_1 保留,然后再次将消息发送出去,重复签名的过程,直到消息的信任值大于或者等于设定的安全阈值时,就认为消息是可信的.这时候当消息的接收者收到消息后就可以只验证最后一次的签名,如果正确就接收该消息,并且在接收之前不会对消息和自己将要发出的消息进行对比也不需要再次签名.以上所有的步骤都是在防篡改元件 TPM 中完成的,由于防篡改元件中的数据是不可以被人工改写的,所以签名及验证过程以及这些过程中所用到的数据是不能够被人工篡改的,所以不必担心车辆恶意修改自己的信任值.对于个人车辆发出的信息也采用上述方法进行处理,要考虑不同车辆在发送消息的过程中对隐私保护的需求不同,特别是私人车辆需要不断变换假名对消息进行签名,来保证安全,具体过程如图 5 所示.

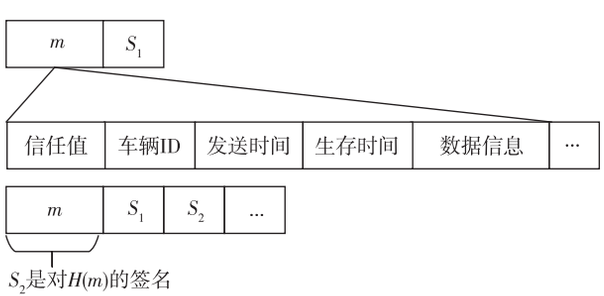

图 5　数字签名的方法

Fig. 5　Method of digital signature

3　安全性分析

3.1　车辆的匿名性

私人车辆在车辆管理中心(DMV)进行注册的过程中就被分配了许多假名和假名证书,存储在车辆的防篡改元件 TPM 中.这些假名和假名证书需要定期更换,车辆每隔半年左右就需要到车辆管理中心去保养以及更换假名,而且每一次签名和前一次签名使用的假名都不相同,在签名的过程中就可以保证自己的真实身份不被泄露.另外一些有特殊需要的公用车辆也可以要求分配假名证书,因此保证了车辆的匿名性.

3.2　消息的完整性和可认证性

车辆在信息传递的过程中,每一次传递信息都会对信息重新进行一次签名,也只有合法的用户才会产生对消息的合法签名,如果不法用户对消息进行了篡改,在验证签名的过程中就不能得到相应的消息摘要的值,如果发现消息被篡改了就停止继续传播.

私人车辆要发送消息 m,首先在 TPM 中会对消息的信任值 Sec 进行累加,然后计算消息的哈希值 $H(m)$,使用 DMV 分配的私钥 $SK_{\mathrm{OBU}}(d,N)$ 对发送的消息进行签名,签名的过程为 $s=(H(m))^d \bmod n$,当车辆在道路上行驶的过程中收到其他车辆发来的签名消息时,首先要对 Sec 的值进行判断,然后对消息进行签名,因为

$$h=s^e \bmod n=((H(m))^d)^e \bmod n=$$
$$(H(m))^{de} \bmod n=H(m),$$

所以 $h=H(m)$ 成立,即如果在消息的传递过程中恶意的攻击者对消息的某一部分进行了篡改,都无法得到正确的哈希值,因此可以保证消息的完整性.

本文中引入了信任值多次累加的方法,由于每一次签名当消息的信任值没有达到安全阈值时,车辆也会通过与自身周围的环境作对比来签发消息然后再进行验证签名,这样可以防止对明显错误的消息进行签名.另外对车辆信任值的不同分类可以提高认证的效率,同时也充分发挥了可信度高的车辆的作用,将消息的多次签名证书和签名摘要信息进行保留也可以防止一个消息被同一个签名者多次签名.当消息达到规定的可信度值的时候,为了保证消息的可靠性,避免中途传递过程中消息被篡改,仍然要通过计算消息的签名来确定消息是否被篡改过,因此该方案可以保证消息的完整性和可认证性.

3.3 消息的可追踪性和不可否认性

当道路环境中出现恶意攻击者频繁地发送虚假信息或者是个别车辆为了自己的利益进行联合攻击时,由于车辆都要在 DMV 进行注册,所以 DMV 可以对违规车辆的签名证书进行查找,并追究相应车辆的责任,其他车辆没有对应假名的消息列表,所以只有 DMV 才可以对违法车辆进行追踪.车辆每一次发送消息时都会将自己的签名证书附加到签名信息字段,因此车辆不可以否认自己发送过的消息.

4 仿真实验

本节对文中所提出的通信协议进行实验仿真并根据最后的仿真结果对本文中的方案进行评估.

4.1 仿真工具的介绍

4.1.1 SUMO 和 MOVE

SUMO 软件始于 2000 年,交通研究组织部门可以通过这一款微观并且开源的道路仿真工具对自己提出的方案进行模拟和评估.

在进行道路交通模拟时需要用 SUMO 生成道路网络,道路网络的生成在 SUMO 中有很多工具共同辅助完成,其中命令行的方式所占的比重最多.主要包括两部分:1)构建道路分布结构;2)道路中车辆移动过程的建立[15].SUMO 中的信息最终存储为 XML 文件,这样可以方便阅读,主要有道路网络文件(*.net.xml)和车辆路径文件(*.rou.xml),车辆的路径文件是由车辆的道路文件辅助生成的.完成了这两部分内容后,就可以借助于 SUMO 进行交通环境的仿真.

使用 SUMO 和 MOVE 可以很容易实现对道路交通状况的部署.通过对车辆的数量、道路的形状、红绿灯、最高限速的设置,可以模拟现实世界中的交通状况.利用 MOVE 生成的交通模拟环境文件是可以在 NS2 中运行的文件.本文使用 SUMO 的版本号是 12.0.3.

4.1.2 NS2

NS2 (Network Simulator version 2)是一种不收费的软件模拟平台[14,16],针对网络技术的代码是公开的.借助于该软件,研究人员可以很方便地开发网络技术,而且从发展现状看,它几乎包含了所有要进行研究的网络技术模块.在车载自组织网络的仿真过程中,使用其中的 IEEE 802.11p 协议进行网络模拟,在 ubuntu12.04 操作系统的环境下,选取了 NS2.35 进行仿真.

4.1.3 SUMO 与 NS2 的耦合

SUMO 作为交通场景仿真模拟的平台,不能对车载自组网(VANET)中的协议进行仿真模拟,因此需要 NS2 网络仿真工具与 SUMO 进行耦合[17].

SUMO 生成的道路交通场景文件可以作为 NS2 中的网络场景配置文件,在 NS2 中可以实现路由协议,SUMO 和 NS2 的耦合过程如图 6 所示.

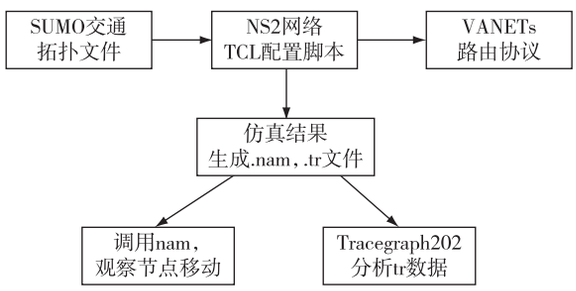

图 6 SUMO 和 NS2 的耦合过程

Fig. 6 Combination of SUMO and NS2

SUMO 的 TCL 脚本要由 SUMO 生成的.net 道路形式文件和随机路径文件.rou 组成.xml 文件,再由 MOVE 工具生成.tcl 文件,编写 NS2 模拟代码.最后进行仿真模拟以及数据的分析.

4.2 实验场景的设置

实验使用了 SUMO,MOVE 和 NS2 工具,车载网选用了如图 7 所示的城市中的道路环境.如图 8 所示的是设有红绿灯的双向 4 车道道路细节.车辆随机地在道路中产生,城市区环境中车辆以 40 km/h 的平均速度行驶.通信过程中的参数如表 2 所示.实验的时间为 675.979 401 3 s,车辆行驶范围的面积是 2 500 m×2 500 m,固定比特率业务流(Constant Bit Rate,CBR)数据包的大小为 512 bit.

图 7 道路环境模拟

Fig. 7 Simulation diagram of urban road

在车载自组织网络中,广播消息是主要的通信

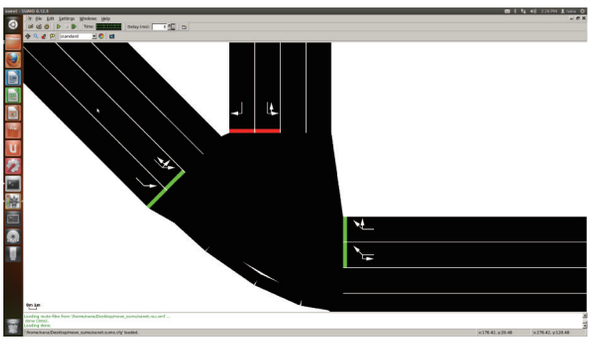

图 8　双向 4 车道模拟

Fig. 8　Simulation diagram for two-way four lanes

方式,NS2 运行过程中的具体参数如图 9 所示.从图 9 中可以观察到天线的高度是 1.5 m,通信距离为 550 m.

表 2　车载自组网络中实验参数设置

Table 2　Experimental parameters in VANET

选项	参数
Vehicle 场景的大小	2 500 m×2 500 m
Simulation time	675.979 401 3 s
Vehicle 数目	随机变换
Vehicle 道路拓扑结构	实际道路
Channel Type	Channel/WirelessChannel
Network Interface Type	Phy/WirelessPhy
Interface Queue Type	Queue/Drop Tail/PriQueue
Antenna Model	Antenna/OmniAntenna
Ad-hoc Routing Protocol	GPSR
Radio Propagation Model	Propagation/TwoRayGround
MAC Type	MAC/802_11
Max Packet in IFO	50
Link Layer Type	LL
Topology Boundary x	652
Topology Boundary x	252

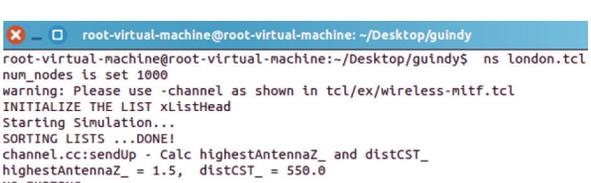

图 9　NS2 的运行情况

Fig. 9　Running process of NS2

如图 10 所示的是 NS2 对 GPSR 协议的模拟过程,图片显示的是运行实验过程中产生的.nam 文件的效果,图 10 中带有编号的小圆圈代表的是车辆节点,这些节点可以在相应的道路上移动,并发送消息,大圆圈代表的是广播消息传送的范围,箭头表示发送的消息.

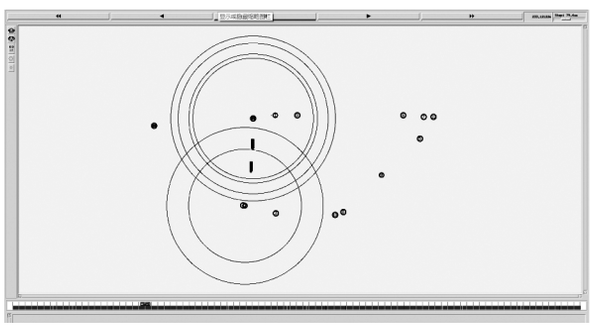

图 10　NS2 模拟

Fig. 10　NS2 simulation result diagram

4.3　性能的评估

为了检测本方案的性能,在本文中,选取了消息的到达率(get ratio)和消息的延迟(message delay)这两个方面来进行分析.

消息的延迟是一个时间量,用来表示将消息从网络的一端传递到另一端的时间.这个时间主要包括发送消息的时延、传播消息的时延、处理消息的时延和消息排队的时延.消息的延迟会对通信造成一定的影响,特别是在车载自组织网络这种通信节点高速移动的网络环境下,要求消息的时延不要过大.如图 11 所示,应用 Tracegraph202 对在 NS2 中运行的.tcl 文件产生的.tr 文件的数据进行分析,发现随着道路上发送消息的车辆不断增加,消息端到端的时延不断增加,而且增长的速率也随着车辆的数目的增加而不断增加.

由于使用广播通信方式,在车载网中传播的消息会很容易发生丢包的现象,车辆在很短的一段时间内可能会收到大量的消息,由于自身的处理能力是有限的,以及受到距离和车速的影响,所以会产生丢包的现象.通过 Tracegraph202 对.tr 文件的分析,对所分析的数据进行整理,本文中主要对消息到达率 GR(其量值为 R_G)进行计算,计算的公式为

$$R_G = \frac{\sum_{i=1}^{i=n} M_{rec}^{i}}{\sum_{i=1}^{i=n} M_{send}^{i}}. \tag{1}$$

下面对其中用到的参数进行解释,n 代表实验环境中车辆节点的数目,M_{send}^{i} 表示车辆 i 发送消息的总数,M_{rec}^{i} 表示车辆 i 收到消息的总数.经过实验分析可以发现,当可以发送消息的实体增多时,整体发送

出去的数据包的数量也会增多,收到的消息的数量也会更多,这也正反映了广播消息的特点.下面根据实验数据,对实验环境中有 50 辆车的情况进行分析,实验具体数据如下:

Simulation length in seconds:675.9794013
Number of nodes:50
Number of sending nodes:50
Number of receiving nodes:50
Number of generated packets:461147
Number of sent packets:460558
Number of forwarded packets:21530
Number of dropped packets:47546
Number of lost packets:53537
Number of sent bytes:80673604
Number of forwarded bytes:11703360
Number of dropped bytes:5113150

对以上数据进行分析,模拟时间为 675.979 401 3 s,点的数目为 50,发出和接收消息的节点数目也是 50,产生的数据包的数目为 461 147,发出的数据包的数目为 460 558,转发的数据包的数目为21 530,丢弃的数据包的数目为 47 546,丢失的数据包的数目 53 537,整个实验过程的消息到达率是 4.675%.表 3 给出了在相同的实验环境下,车辆的数目对车辆发出消息到达率的影响.

表 3 不同车辆数目下封包到达率

Table 3 Arrival ratios for different numbers of vehicle

车辆数/辆	消息到达率/%
50	4.675
100	7.212
200	14.604
300	25.474
400	33.349

最后,将本文提出方案算法的时间效率与文献[18-19]中的隐私保护算法的消息认证时间作对比.表 4 所示为确保消息的可靠性所消耗的时间.在中央处理器主频为 2.39 GHz,内存为 8.00 GB,容量为 256 GB 固态硬盘的环境下,点乘运算消耗时间是 0.6 ms,双线性计算消耗的时间是 4.5 ms,模幂运算消耗的时间是 2.1 ms,中国剩余定理消耗的时间是 6 ms,哈希函数的执行时间是 0.002 ms,由于哈希运算的时间是千分之一数量级的,对最后的运算时间没有特别大的影响,因此可以忽略不计.本文的方案中,假设所有的车辆都是私人车辆的情况下,最多需要执行模幂运算 5 次,与文献[18-19]中的数据进行比较,本文方案的时间效率有所提升.

表 4 计算代价对比

Table 4 Comparison with computation cost

方法	代价
文献[18]	11 次点乘运算+3 次双线性计算(20.1 ms)
文献[19]	6 次模幂+1 次中国剩余定理运算(18.6 ms)
本文	5 次模幂(10.5 ms)

综上所述,本文所提出的协议的方案,既保护了用户的隐私,又满足了不同用户的安全需求以及保证了消息传输的质量.如表 5 所示,统计了不同车辆数目情况下端到端的平均时延的统计数据.如图 11 所示,用折线图画出了不同车辆的平均时延变化以及不同车辆数目下封包到达率的变化情况.从图 11 中可以观察到随着车辆数目的增多,由于需要排队处理的消息在不断地增加,所以消息的平均时延也在不断增长,同时消息的封包到达率也在不断地增长,主要是由于车辆数目的增长,接受消息的车辆也随之增加.

表 5 不同车辆数下端到端的平均时延

Table 5 Average delays for different numbers of vehicle

车辆数/辆	端到端平均时延/s
50	4.579
100	20.890
200	65.372
300	175.43
400	421.90

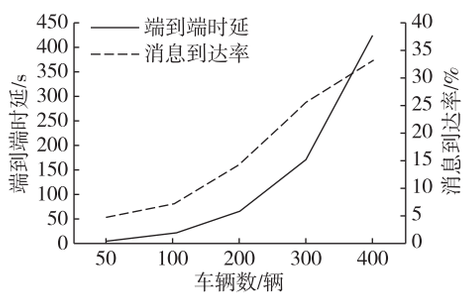

图 11 不同车辆下的平均时延变化及封包到达率

Fig. 11 End to end delays and message arrival ratios for different numbers of vehicle

5 结束语

通过对安全阈值的设定和信任值的累加,可以

有效防止车辆因为盲目的信任公用车辆而导致交通事故,不仅可以有效地提高安全性,还可以抵抗联合攻击.本方案中,公共车辆也可选择适合自己的签名方案,因此可以携带少量的假名,节约存储空间.消息每一次签名都对前一次的签名结果进行保留,这样可以防止消息的篡改和对一条消息的重复签名.在本文的车载自组网认证方案中,增加了认证方案的灵活性和认证的效率.在未来的研究工作中,要根据车辆是否遵守规则,来对信任值的大小进行增减,从而来鼓励驾驶员文明驾驶.

参考文献

References

[1] Chim T W,Yiu S M,Hui L C K,et al.SPECS:Secure and privacy enhancing communications schemes for VANETs[J].Ad Hoc Networks,2011,9(2):189-203

[2] Lin X D,Lu R X,Zhang C X,et al.Security in vehicular ad hoc networks[J].IEEE Communications Magazine,2008,46(4):88-95

[3] 陆杰.车载自组网中隐私保护关键技术研究[D].镇江:江苏大学计算机科学与通信工程学院,2016
LU Jie.Research on privacy protection in vehicular Ad-hoc network[D].Zhenjiang:School of Computer Science and Telecommunication Engineering, Jiangsu University,2016

[4] Aijaz A, Bochow B, Dötzer F, et al. Attacks on inter-vehicle communication systems: An analysis[J]. Proc Wit,2006:189-194

[5] Basagni S,Conti M,Giordano S,et al.Mobile Ad hoc networking:Cutting edge directions[M].2nd ed.Piscataway, NJ:IEEE Press,2013

[6] 高永康,郝建军.车载自组网中的网络与信息安全[J].中兴通讯技术,2011,17(3):21-23
GAO Yongkang, HAO Jianjun. Network and information security in vehicular Ad hoc networks[J].ZET Communications,2011,17(3):21-23

[7] 甄伟娜.车载自组网的认证和隐私保护研究[D].北京:北方工业大学理学院,2016
ZHEN Weina.The research of vehicle ad hoc network authentication and privacy protection[D].Beijing:College of Science,North China University of Technology,2016

[8] 陆杰,徐宗保,周从华.车载网中基于假名验证公钥的批量认证方法:中国,2014-12-11[P].2015-03-04
LU Jie,XU Zongbao,ZHOU Conghua.The batch authentication method based on pseudonym verified public key in vehicle ad hoc network: China, 2014-12-11[P]. 2015-03-04

[9] 刘辉.车载自组织网络信息认证和隐私保护机制的研究[D].西安:西安电子科技大学通信工程学院,2012
LIU Hui.A study of message authentication and privacy preservation in vehicular ad hoc networks[D].Xi'an: School of Telecommunications Engineering,Xidian University,2012

[10] 徐甜,宋强.基于代理盲签名的车载自组网认证技术研究[J].科技通报,2012,28(10):170-173
XU Tian, SONG Qiang. Research of an authentication scheme based on the proxy blind signature scheme for the vehicular Ad-hoc networks[J].Bulletin of Science and Technology,2012,28(10):170-173

[11] 张新运,许艳,崔杰.车载网中基于无证书签名的匿名认证协议[J].计算机工程,2016,42(3):18-21
ZHANG Xinyun,XU Yan,CUI Jie.Anonymous authentication protocol based on certificateless signature for vehicular network[J].Computer Engineer,2016,42(3):18-21

[12] Capkun S,Hubaux J P.Secure positioning of wireless devices with application to sensor networks[C]//24th Annual Joint Conference of the IEEE Computer and Communications Societies,2005,3:1917-1928

[13] Huang J L,Yeh L Y,Chien H Y.ABAKA:An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J].IEEE Transactions on Vehicular Technology, 2011, 60(1): 248-262

[14] 魏艳娜,刘雪丽.基于 RSA 的数字签名体制研究[J].北华航天工业学院学报,2014,24(5):20-22
WEI Yanna,LIU Xueli.Research on digital signature system based on RSA[J].Journal of North China Institute of Aerospace Engineering,2014,24(5):20-22

[15] Peng Y,Abichar Z,Chang J M.Roadside-Aided Routing (RAR) in vehicular networks[C]//IEEE International Conference on Communications,2006,8:3602-3607

[16] Issariyakul T, Hossain E. Introduction to network simulator NS2[M].New York:Springer,2012:21-40

[17] 王腾飞.基于 NS2 的车载自组织网络仿真技术研究[D].武汉:武汉理工大学计算机科学与技术学院,2013
WANG Tengfei.Research on simulation technology of vehicular ad hoc networks based on NS2[D].Wuhan: School of Computer Science and Technology,Wuhan University of Technology,2013

[18] Zhang C X,Lu R X,Ho P H,et al.A location privacy preserving authentication scheme in vehicular networks[C]//IEEE Wireless Communications and Networking Conference,2008:2543-2548

[19] 郭松矗.VANET 下保护位置隐私查询和匿名认证的研究[D].合肥:安徽大学计算机科学与技术学院,2013
GUO Songchu. Research on location privacy-preserving querying and anonymity authentication in VANET[D]. Hefei: School of Computer Science and Technology, Anhui University,2013

南京信息工程大学学报(自然科学版),2017,9(5):480-489
Journal of Nanjing University of Information Science and Technology(Natural Science Edition),2017,9(5):480-489

Privacy protection scheme for VANET based on urban vehicle classification

ZHAO Jia[1,2] LI Na[1,2] HAN Lei[3] LIU Jiqiang[1,2]

1 Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044

2 School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044

3 Unit 66019 of PLA, Beijing 102212

Abstract The Vehicular Ad Hoc Network (VANET) enhances the traffic efficiency and improves the traffic environment, however, it brings up security threats such as information tampering, forgery, as well as privacy disclosure. Thus, the message authentication scheme consistent with characteristics of the VANET is in urgent need. In this paper, we take the option of privacy protection scheme for VANET based on vehicle classification in urban transport system, which includes classification and assignment of trust values for different types of vehicles. For private vehicles, a pseudonym multiple signature scheme is employed to sign the message; while for the public vehicles and RSUs without identity privacy protection requirement, we can use the RSA signature scheme to sign messages. At the same time, the signature is required to accumulate the trust value of the strategy to improve the message reliability. Finally, SUMO, MOVE and NS2 are employed to jointly simulate the proposed scheme, and the result shows that the scheme is more flexible and less time-consuming compared with other schemes proposed in references of[19-20].

Key words classification of vehicles; privacy protection; trust value measure; pseudonym