文章编号：2095-2163(2021)04-0005-05 中图分类号：TP309.2 文献标志码：A

面向 V2X 安全通信的认证协议研究

吴甜甜，杨亚芳，赵运磊
（复旦大学 计算机科学技术学院，上海 200433）

摘 要： 车联网作为提高交通效率和安全最有前途的技术之一，已经引起了工业界和学术界的广泛关注。其中，V2X 安全通信是研究热点之一。然而，V2X 技术的发展也引发了许多安全和隐私问题。为了解决这些问题，大量面向 V2X 通信的认证协议被提出。本文首先详细介绍了 V2X 通信的标准模型以及车联网的特点，并根据其特点分析了认证协议设计中需要满足的安全需求；对近几年的 V2X 认证协议进行了分类，并分析了各类协议的优缺点；讨论了面向 V2X 通信的认证协议的未来研究方向。

关键词： 车联网；V2X；认证协议

Research on Authentication Protocol for Secure V2X Communication

WU Tiantian, YANG Yafang, ZHAO Yunlei
(School of Computer Science, Fudan University, Shanghai 200433, China)

【Abstract】 As one of the most promising technologies for improving traffic efficiency and safety, the VANETs have attracted widespread attention from both industry and academia. Among them, V2X secure communication is one of the research hotpots. However, the introduction of V2X communication technology also raises a number of security and privacy concerns. To address these problems, many V2X secure communication authentication have been proposed. In this paper, we first introduce the standard model of V2X communication and the characteristic of the VANETRs in detail, and analyzes the security requirements that need to be meet in the design of the authentication protocol according to the characteristics of VANETs. Then, we classify the V2X authentication protocols proposed in recent years. We also discuss the future research directions of V2X authentication protocol.

【Key words】 VANETs; V2X; Authentication Protocol

0 引 言

近年来，由于经济的发展，全球的汽车保有量呈逐渐增长的趋势，车联网（VANET）的产业化和普及对于中国构建和谐的汽车社会具有重要的意义[1-2]。但车联网 V2X 通信中的隐私泄露等安全问题严重阻碍了其应用落地。在 V2X 通信中，车辆在行驶过程中，需要定期生成安全信息发送给其他车辆或设备。附近的车辆可以根据收到的交通信息及时做出反应来避免交通混乱。在这种情况下，如果攻击者对消息进行篡改、冒充其它车辆发送信息或是发送虚假信息都会造成严重的交通事故及人员伤亡。因此，设计出面向 V2X 安全通信的车联网认证协议是亟待解决的问题。

1 V2X 通信模型及安全需求

1.1 V2X 通信标准系统模型

车用无线通信技术（V2X，Vehicle to Everything）是将车辆与其他一切事物连接通信的技术。其中，V 表示车辆，X 表示任何与车辆交互的对象，包括车、人、路侧基础设施等。标准的 V2X 通信系统模型如图 1 所示。主要包括以下几种实体：智能网联汽车、路侧基础设施、行人和网络。

V2X 的通信模式主要包括：车车通信（V2V，Vehicle to Vehicle）、车路通信（V2I，Vehicle to Infrastructure）、车人通信（V2P，Vehicle to Pedestrian）、车网通信（V2N，Vehicle to Network）。

V2V 指的是车辆之间进行通信，一般用于传输车辆实时获取的周围车辆的速度、位置、行为等信息。V2V 可以应用于车辆的监督管理，避免或减少交通事故的发生。V2I 通信指的是车辆与路测基础设施（如交通信号灯、摄像头、路侧单元等）进行通信。V2I 通信可应用于实时信息服务和城市交通监管等。V2P 指的是车辆和行人持有的电子设备进行通信，主要用于信息服务。V2N 指的是车辆与接入网络的云平台进行通信，可用于车辆导航、远程监

基金项目：国家自然科学基金（61877011）。

作者简介：吴甜甜（1996-），女，硕士研究生，主要研究方向：车联网应用密码、安全协议；杨亚芳（1994-），女，博士研究生，主要研究方向：密码学、车联网安全；赵运磊（1974-），男，博士，教授，主要研究方向：后量子密码、密码协议和计算理论。

收稿日期：2020-12-15

控、紧急救援等场景。

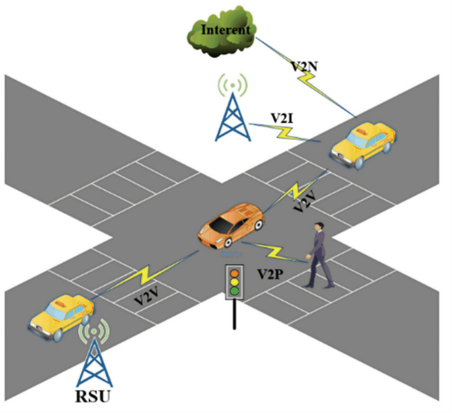

图 1 V2X 系统模型

Fig. 1 System model of V2X

1.2 车联网特点

车联网除了具备 MANET 的一些基本特点,同时也具备自己的独特属性。主要可以概括为以下几点:

(1)自组织性。在 V2V 通信中,各组成节点是移动中的车辆,各车辆根据需求自发地加入到网络中,整个网络没有中心节点。对于每辆汽车,其在网络中的权利和优先级是等同的。根据不同的应用场景,在某些 V2I 场景中,部分路侧单元(Roadside Unite,RSU)可能担任中心节点的角色。

(2)网络拓扑结构动态变化。由于车辆的快速移动,对于某区域来说是迅速进入或退出,整个网络的拓扑结构呈现一个不断变化的状态。因此,在制定各类车联网解决方案时,除了针对一般网络特点做出考虑之外,不可忽视其动态变化的网络拓扑结构。

(3)无限的网络规模。车联网的实现可以在一个城市内,也可以是几个城市甚至是几个国家内。这意味着,车联网的网络规模在地理上是不受限制的,即车联网具有无限的网络规模。

(4)移动轨迹可预测。移动的汽车虽然移动速度较快,但由于受到移动方向以及公路条件等限制,对于系统管理者而言,在较短的时间内,所有移动车辆确定了移动方向的前提下,移动轨迹是可预测的。

(5)快速的信息交换。在 V2V 和 V2I 的通信模型中,移动中的车辆均需向附近的节点阶段性地发出通信信息,并接收来自附近节点的通信信息。由于车辆的通信信息具有时效性,且移动速度过快,因此要求通信时延低。

(6)安全需求高。移动的车辆需要动态的发送移动中的各种数据,这些数据对于安全性需求较高。如果网络中存在的恶意节点对安全信息进行窃听、伪造、篡改,可能造成严重的安全事故,对用户生命财产安全造成威胁。

1.3 安全需求

为了实现安全的 V2X 通信,应当根据车联网特有的特性,设计满足一些特殊的安全特性的认证协议。主要包括以下几点:

(1)可用性。要求在通信中具有高连接性和足够的带宽,来保证通信的流畅。网络必须保证在需要的时间内保持可用,必须对特定的应用具有很快的响应速度。因此即使是毫秒级的延时,都可能使发送的信息失去时效性。

(2)可认证性。车联网中被授权的合法节点可以通过网络接收和发送信息。在该过程中,必须对其中的节点进行身份认证。认证过程包括:验证发送者的身份是否合法、实际发送方是否与其声称的身份一致,以及是否被授权发送信息。

(3)完整性。接收方在接收信息后,为了信任所接收的消息内容,需要对消息进行验证,保证消息未被篡改。也就是说,接收到的消息与发送方发送出的消息应当是相同的。经过攻击者篡改或者伪造的消息,应被接收方拒绝。

(4)不可否认性。发送方可能发出错误的消息,攻击者可能发送出虚假消息,这些可能对系统的安全造成威胁。不可否认性要求,对于发送者而言,其发送出的任何消息都不可否认曾经发送过。

(5)隐私保护。车联网中发送的消息大多数是在公共信道中进行传输的,这意味着攻击者可能对发送的信息进行窃听。隐私保护要求,通过公共信道传输的信息不应暴露发送方和接收方的秘密信息。包括车辆的真实身份信息、位置信息、密钥等。

(6)不可链接性。不可链接性要求,即使攻击者获取到同一车辆发送出的不同的消息,也无法确定这些消息的来源是否为同一车辆,不能通过对消息进行分析定位到该车辆并对其进行追踪。

(7)可追溯性。当系统中存有纠纷的信息需要进行追责时,需要经过授权的中心机构来对信息进行解析,从而确定发送者的真实身份。可追溯性意味着中心机构 TA 可以通过传输信息确定发送者的真实身份,并对其进行后续操作。

2 车联网认证协议

为了解决 V2X 的安全通信问题,大量的认证协议被提出。本文仅介绍几种主要的认证协议。

2.1　基于对称密码的认证协议

使用 MAC 码进行消息认证的对称密码，具有很高的计算效率和较低的通信负载。发送方使用共享密钥为每个消息生成 MAC 码。在匿名集中的所有用户均使用相同的密钥，可以对消息的 MAC 码进行验证。

2005 年，Choi 等人首次提出了基于对称密码的车联网认证协议[3]。在该协议中，授权机构为每个车辆发送唯一的标识符和一个种子，用于生成不断更新的假名。用于验证的密钥在所有的 RSU 和车辆中是共享的。2007 年，文献[4]提出的协议中，车辆在没有中央授权的情况下保留用于认证的随机密钥集，以便在零信任策略下保护用户的隐私。该协议的匿名性是通过在不同随机集之间共享密钥来实现的。

基于对称密码的认证协议中存在两个问题：一是 VANET 中的密钥管理问题，不仅容易受到攻击，并且会导致通信和存储的开销。其次，该类协议缺乏不可否认性，无法为每辆车都提供认证。2016 之后的此类协议[5-7]，提出了双重认证和密钥托管技术，用于解决上述问题。双重认证机制不仅可以提供更高的安全性，防止未授权的车辆进入到网络中，同时双重认证的群组密码管理机制，可以有效地将群组密钥分发给所有成员。

2.2　基于公钥密码的认证协议

在基于公钥密码（PKI）的认证协议中，车辆配备了用于匿名通信的公私钥对。证书管理机构（CA）颁发公钥证书，用于车辆的身份验证，其中包含了车辆的公钥以及证书机构生成的数字签名。车辆使用私钥和假名对传输的信息生成签名。接收方可以通过签名和证书来验证消息来源的可靠性，在此过程中并不会暴露发送方的身份隐私。

CA 负责长期证书的颁发和管理。在文献[8]提出的方案中，车辆以一定的间隔从 CA 处获得短期假名。为了减少与 CA 通信的开销，文献[9]提出的方案允许车辆可以自行生成假名。2012 年，Lu 等提出假名更新策略[10]，通过限制假名的使用寿命防止车辆被跟踪。撤销假名证书带来的巨大开销是公钥密码体制中面临的难题，这项工作大多是通过证书撤销列表（CRL）来完成的。如果车辆的长期证书被撤销，将不能从 CA 处获取到新的假名。文献[11-12]中提出了几种可扩展的 CRL 分发方法，但并不能阻止车辆在所有假名过期之前继续通信。为了避免公钥密码体制中繁重的证书撤销问题，基于身份的认证协议应运而生。

2.3　基于身份基签名的认证协议

身份基签名（IBS）使用节点的身份作为公钥，使用基于身份生成的私钥来对发送的消息进行签名。相比于公钥密码体制，仅使用发送方的身份完成消息签名的验证，减少了证书的管理和存储开销。在 IBS 中，私钥生成器（PKG）可看作可信任第三方用于私钥的生成和管理。

2001 年，Boneh 等[13]人基于椭圆曲线上的双线性配对，提出了第一个基于身份的加密方案。为了减少 VANET 中 IBS 方案的计算开销，Lu 等[14]在 2012 年提出了一种名为 IBOOS 的新型认证框架，实现了基于身份的在线和离线签名。在改进版的 IBOOS[15]中，签名过程被分解为在线和离线阶段。由于加速了配对过程，签名验证的效率也得到了很大的提高。

与传统的 PKI 相比，IBS 消除了对公钥验证的证书要求。因此不需要为公钥分配证书。同时，IBS 避免了管理证书撤销列表的繁重开销。但是，IBS 中的所有私钥都是由 PKG 生成的。这意味着在 VANET 中，PKG 会知道所有车辆的私钥，产生密钥托管的问题。为了解决密钥的托管问题，文献[16]中提出了一种分布式聚合隐私保护的认证协议（DAPPA），该协议中包含多个可信任第三方机构（TA）。根 TA 负责产生系统参数，并为 RSU 颁发相应的证书。在授权期间，车辆会生成一次性的私钥和基于身份的一次性聚合签名。DAPPA 使用根 TA 未知的一次性私钥，解决了托管问题。文献[17]提出了一种名为 IFAL 的支持可证明安全的适用于 V2V 和 V2I 的隐私保护方案，引入了一种新型的密码机制，同时可以避免证书撤销的开销，支持车辆的间歇性连接。

2.4　基于无证书签名的认证协议

为了消除基于 PKI 的方案中昂贵的证书管理问题和 IBS 中的密钥托管问题，AI-Riyami 等[18]于 2003 年首次提出了无证书公钥机制（CLS）。与 PKI 方案不同，无证书方案在不需要证书的前提下，仍然可以确保公钥的真实性。在无证书方案中，密钥生成中心（KGC）充当半可信任的第三方，负责向用户提供根据用户身份计算出的部分私钥，用户可以使用自己选取的部分私钥和 KGC 生成的部分私钥生成自己的完整私钥。最后，用户使用公共参数和秘密值生成公钥。与 IBS 方案不同的是，KGC 无法获取用户的完整私钥。

近年来，几种改进的无证书短签名（CLSS）被提

出并应用到 VANET 中。2015 年,文献[19-20]提出了新的基于 CLSS 的 V2I 通信无证书聚合签名方案。通过将车辆广播的消息映射到伪身份来实现条件隐私保护。当发生争议时,授权机构可以从任何伪身份中检索出真实身份。由于 CLSS 在 VANET 中的部署严重依赖于配对的有效实现,提出了许多关于硬件加速器的研究方案[21-22],极大提高了 CLSS 的效率。因此,CLSS 在 VANET 的应用中是一种很有前景的隐私保护认证协议。

3 研究展望

面向 V2X 安全通信的车联网认证协议,一直是车联网安全的重要研究方向之一,这对于车联网的应用落地具有非常重要的意义。然而,车联网相关设备的计算和存储等各类资源有限,认证协议需要满足的功能需求却很多。因此,设计出安全高效的认证协议是需要解决的技术难题。本文对未来车联网认证协议研究领域的发展方向总结如下:

(1)轻量级。由于车联网中的主体是移动汽车,其存储能力和计算资源有限,设计出轻量级的通信协议是解决资源受限的关键。现有认证协议大多数是基于椭圆曲线或双线性配对设计的,计算开销和通信开销均较高。对于轻量级协议的设计而言,一方面,现有针对 V2X 通信的算法可以进一步优化;另一方面,可以对现有轻量级算法在车联网环境中的应用进一步研究。

(2)相互认证。现有的认证协议大多数只能实现单方面认证,即接收方对消息来源进行认证,不能实现通信双方的相互认证。然而,相互认证是必须面对的问题。在 V2X 通信中,从安全的角度考虑,实现通信双方的相互认证是必要的,可以避免更多冲突的发生。设计出具有相互认证功能的通信协议是未来研究的重点方向之一。

(3)去中心化。现有的认证协议中,大多存在可信任的第三方完成密钥分发以及认证等功能。事实上,信任机制很难保证。因此,设计出去中心化的认证协议,是 V2X 通信未来发展的一个重要方向。区块链等新兴技术的出现,或许会为去中心化认证协议的设计提供新的研究思路。

4 结束语

随着智能网联汽车的普及,面向 V2X 通信的认证协议会成为车联网安全领域重要的研究方向之一。本文详细介绍了车联网 V2X 通信模型,针对其特点提出了协议设计需要满足的安全需求。针对国内外的研究现状,分类介绍了现有的认证协议,总结了最新的研究进展。最后提出了面向 V2X 通信的车联网认证协议未来的发展方向。本文以其为初入车联网领域的研究者提供参考。

参考文献

[1] 唐刚. 车联网安全:持续监测和远程检测是关键[N]. 人民邮电, 2020-08-12 (3).

[2]《国家车联网产业标准体系建设指南(车辆智能管理)》解读[J]. 道路交通管理,2020(7):50-51.

[3] CHOI J Y. Balancing auditability and privacy in vehicular networks [C]// Q2SWinet'05 - Proceedings of the First ACM Workshop on Q2S and Security for Wireless and Mobile Networks, 2005:79-87.

[4] XI Y, SHA K, SHI W, et al. Enforcing Privacy Using Symmetric Random Key - Set in Vehicular Networks [C]// International Symposium on Autonomous Decentralized Systems, 2007:344-351.

[5] VIJAYAKUMAR P, AZEES M, KANNAN A, et al. Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks [J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 1-14.

[6] VIJAYAKUMAR P, AZEES M, CHANG V, et al. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks[J]. Cluster Computing, 2017,20(3):2439-2450.

[7] HAKEEM S A A, EL-GAWAD M A A, KIM H W. A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks[J]. IEEE Access, 2019, (99):1-1.

[8] EICHLER S. Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility [C]// Intelligent Vehicles Symposium. IEEE, 2007:541-546.

[9] ZENG K. Pseudonymous PKI for Ubiquitous Computing.[C]// Public Key Infrastructure, Third European Pki Workshop: Theory & Practice, 2006:207-222.

[10] LU R, LIN X, LUAN T H, et al. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs[J]. IEEE Transactions on Vehicular Technology, 2012, 61(1):86-96.

[11] KONDAREDDY Y, CRESCENZO G D, AGRAWAL P. Analysis of Certificate Revocation List Distribution Protocols for Vehicular Networks[C]// Global Telecommunications Conference. IEEE, 2010:1-5.

[12] VIJAYAKUMAR P, CHANG V, DEBORAH L J, et al. Computationally Efficient Privacy Preserving Anonymous Mutual and Batch Authentication Schemes for Vehicular Ad Hoc Networks [J]. Future Generation Computer Systems, 2016, 78.

[13] BONEH D, FRANKLIN M. Identity-Based Encryption from the Weil Pairing[C]// Annual International Cryptology Conference, 2001:213-229.

[14] LU H, LI J, GUIZANI M. A novel ID-based authentication framework with adaptive privacy preservation for VANETs[C]// 2012 Computing, Communications and Applications Conference. IEEE, 2012: 345-350.

(下转第 13 页)