

一种 VANET 条件隐私保护消息认证方法

张盼盼, 沈明玉, 周 健

(合肥工业大学 计算机与信息学院, 安徽 合肥 230009)

摘 要: 提出了一种 VANET 条件隐私保护消息认证(CPMA)的方法, 采用分级认证技术, 使用加密的 Hash 消息认证码(HMAC)进行证书吊销检查, 减少了计算量, 在保证安全性的前提下可以显著地减少消息认证延迟. 仿真实验结果和分析表明了方法的有效性.

关键词: 车载网; 隐私保护; 消息认证; 证书吊销列表

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2014)10-0094-04

A Conditional Privacy-preserving Message Authentication Algorithm in VANET

ZHANG Pan-pan, SHEN Ming-yu, ZHOU Jian

(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: This paper proposed a Conditional Privacy-preserving Message Authentication (CPMA) algorithm. CPMA adopted hierarchical authentication technology and encryption Hash Message Authentication Code(HMAC) to check revocation certification. This algorithm reduce calculating complexity and the message authentication delay without compromising security. Simulation analysis and results show the effectiveness of CPMA algorithm.

Key words: Vehicle Network; privacy-preserving; message certification; Certificate Revocation List (CRL)

1 引言

车载自组织网络^[1] (Vehicular Ad Hoc Network, VANET)是一种自组织、结构开放的、车辆间通讯的网络, 主要用于道路交通信息服务和辅助安全驾驶等领域.

通信分为 2 个部分: 车-车(vehicle to vehicle, V2V)通信和车-基础设施(vehicle to infrastructure, V2I)通信.

车辆通信过程中, 用户将面临隐私信息泄露、隐私权被侵害的危险, 因此需要进行隐私保护. 隐私通常包括^[2]: (1)身份隐私. 即车主的真实身份, 包括驾驶证号、姓名、身份证等信息; (2)服务隐私; (3)位置隐私. 包含 V2I 通信隐私和 V2V 通信隐私.

目前, VANET 隐私保护主要通过部署公共密钥基础设施(PKI), 使用假名和证书吊销列表

(CRL)的证书管理授权机制, 实现车辆匿名通信、隐藏车辆信息或模糊车辆身份等. 文献[3]中提出了基于证书的安全通信协议(CBCP), Lin 等人提出了基于群签名的方案(GSB)^[4], 文献[5]中采用基于加密 mix-zone(车辆混合区域)方法替代传统的暂停通信更换假名的方法, 这些方法提高 VANET 的安全性, 但增加了处理的复杂度.

本文针对检查吊销列表 CRL 耗时过多的问题^[4], 提出了一种 VANET 条件隐私保护消息认证(CPMA)方法, 采用基于 Hash 消息认证码的分级吊销检查方法, 可以有效减少检查吊销列表的时间、降低认证延迟.

2 相关技术背景

2.1 双线性对

双线性配对函数通常被用在密码分析中, 通过

使用配对函数,可以将某些椭圆曲线上的离散对数问题约减到有限域上的离散对数问题。

设 G_1 和 G_2 分别是阶为素数 q 的加法循环群和乘法循环群, P 是 G_1 的一个生成元. $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对。

(1) 双线性:

$$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{a \cdot b} = \hat{e}(Q, P)^{a \cdot b}$$

对所有的 $P, Q \in G_1, a, b \in Z_{q^*}$ 。

(2) 非退化: 存在 $(P, Q) \in G_1 \times G_1$, 使得 $\hat{e}(P, Q) \neq 1$, 其中, 1 表示乘法群 G_2 中的单位元。

(3) 对称: $\hat{e}(P, Q) = \hat{e}(Q, P)$, 对所有的 $P, Q \in G_1$ 。

(4) 可计算性: 映射 $\hat{e}$ 是高效可计算的。

给定阶数 q 的椭圆曲线上的点 P 和点 Q , 椭圆曲线离散对数问题(ECDLP)^[6] 的计算取决于计算满足 $1 \leq l \leq q-1$ 和 $Q = lP$ 的正整数 l 。

2.2 哈希链

本文方法采用哈希链生成证书的版本号, 有效防止前向攻击。哈希链是将哈希函数 $h(x)$ 循环地用于一个字符串(即将所得哈希值再次传递给哈希函数得至其哈希值)。设有哈希链的初始值 $u, v_j = h(v_{j-1}), \forall 1 \leq j \leq n$, 如图 1 所示。

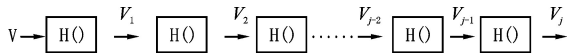


图 1 哈希链

2.3 搜索算法

吊销证书列表 CRL 搜索主要用于查找证书是否有效, 若能在 CRL 中找到匹配证书, 则说明该证书无效, 否则为有效。最常见的搜索算法^[7]包括线性搜索、二进制搜索。线性搜索是把每个实体证书和 CRL 中的证书做比较, 如果匹配, 该证书被吊销, 反之亦然。二进制搜索是每个 OBU 把接收到的吊销证书排序后放在有组织的吊销证书缓冲区内, 类似折半查找。

3 分级认证与证书吊销

3.1 分级认证架构

本文采用了四种网络组件: MA(master authority)、TA(trusted authority)、RSU 和 OBU。网络结构和各个层次之间的关系, 如图 2 所示。

MA 位于四层模型的最顶层, 是证书发放的认证中心, 负责 TA 的注册。TA 位于第二层, 负责 RSU 和 OBU 的注册。RSU 位于第三层, 能与 TA 及 OBU 通信。OBU 位于最底层, 是被认证的对象。

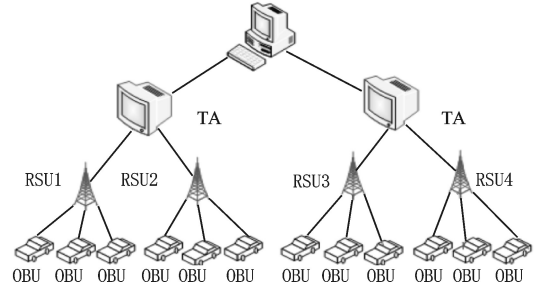


图 2 分级认证架构

具体的隐私保护处理流程如图 3 所示。

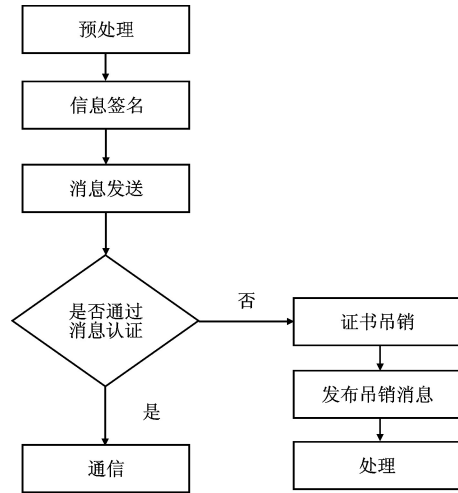


图 3 处理流程

3.2 预处理

① TA_x (TA_x 表示第 x 个 TA) 向 MA 发送证书请求, 得到由 MA 颁发的主密钥集 $k_{xi} = \{K_{xi} \mid K_{xi} \in Z_{q^*}, 1 \leq i \leq n\}$, (Z_{q^*} 是有理数, n 为密钥数) 和 MA 的一对密钥 MK^+ 和 MK^- 。 TA_x 计算自己的私钥池 U_{xs} 和公钥池 U_{xp} :

$$U_{xs} = \{k_{xi} * Q \mid 1 \leq i \leq l\} \in G_1$$

$$U_{xp} = \{P/k_{xi} \mid 1 \leq i \leq l\} \in G_1$$

G_1 是阶为素数 q 的加法循环群, $MK^+, MK^- \in G_1$ 。

② RSU 向其父节点 TA_x 发送证书请求, 获得 TA_x 传递的 MA 的一对密钥 MK^+ 和 MK^- 。

③ OBU_a 通过 RSU 向 TA_x 发送证书请求, TA_x 将自己的公钥 K_g , 生成假名的函数 H , 密钥的更新规则 f 及匿名证书发送给 OBU_a :

$$PID_a(t) = H(ID_a, t)$$

$$SK_{a-ver+1} = f(SK_{a-ver}, PK_{a-ver+1}) \in U_{xs}$$

$$CERT(PID_a, PK_a, MK^+, sig_{TA_x}(PID_a || SK_a))$$

其中 $K_g \in G_2$ (G_2 是阶为素数的乘法循环群),

PID_a 是车辆使用的一种随时间动态更换的假名。 ID_a 是 OBU_a 的真实身份, t 表示假名的开始时间 t_1 和有效时长 t_2 的二维表。 SK_{a-ver} 为 OBU_a 证书版本号为 v_{a-ver} 时的私钥, $PK_{a-ver+1}$ 为 OBU_a 证书版本号为 $v_{a-ver+1}$ 时的公钥, $f(SK_{a-ver}, PK_{a-ver+1})$ 为 OBU_a 与 TA_x 约定的新私钥的生成规则。 MK^+ 是 MA 的公钥, $PK_a \in U_{xp}$, $SK_a \in U_{xs}$, $sig_{TA_x}(PID_a || SK_a)$ 是 TA_x 的签名。

3.3 消息签名和认证

3.3.1 OBU_a 消息签名

OBU_a 消息签名的步骤:

① 计算哈希消息认证码 HM_{check}

$HM_{check} = HMAC(K_g, MK^+, PID_{a-ver} || T_{stamp})^2$ 其中 PID_{a-ver} 是 OBU_a 证书版本号为 v_{a-ver} 时的假名, T_{stamp} 是时间戳, K_g 是初始共享的 TA_x 公钥, MK^+ 是 MA 的公钥。

② 根据 HM_{check} 生成报文 M

$M = (m || T_{stamp} || CERT_{a-ver}(PID_{a-ver}, PK_{bi}, MK^+, sig_{TA_x}(PID_{a-ver} || SK_{a-ver})) || sig_a(m || T_{stamp}) || HM_{check})$

其中 m 为要广播的消息, $CERT_{a-ver}$ 、 SK_{a-ver} 分别表示 OBU_a 证书版本号为 v_{a-ver} 时的匿名证书和私钥, PK_{bi} 是 OBU_b 的第 i 个公钥, $sig_a(m || T_{stamp})$ 是 OBU_a 的签名。

③ 向 OBU_b 发送 (HM_{check}, M)

$(HM_{check}, M) \rightarrow OBU_b$

3.3.2 OBU 消息认证

OBU_b 收到同一 RSU 范围内 OBU_a 的消息认证的步骤:

① 计算 $HMAC(K_g, MK^+, PID_{a-ver} || T_{stamp})^2$, 若结果与收到的 HM_{check} 不一致, 则丢弃报文 M , 转 ④;

② 分别验证 $sig_{TA_x}(PID_{a-ver} || SK_{a-ver})$ 、 $sig_a(m || T_{stamp})$ 及 $CERT_{a-ver}$, 若验证不通过则认为报文 M 中的消息 m 无效, 丢弃报文 M ;

③ 消息验证通过, 结束。

④ 未通过消息验证, 结束。

一般情况下, 不同 RSU 范围内 OBU 之间的通信需要相应的 TA 甚至是 MA 的协调。

3.4 TA 负责 OBU 证书吊销及发布

3.4.1 证书吊销

TA_x 吊销证书有两种情况:

主动式: 即 OBU_a 主动发送更新证书的请求, TA_x 动态更新其证书。

被动式: 即 OBU_a 不主动发送更新证书的请求, TA_x 根据 OBU_a 证书的发布日期计算有效期, 若超过有效期, 则动态更新其证书。

TA_x 吊销和更新证书的步骤:

① OBU_a 最近一次被吊销的证书版本号为 v_{a-ver} , 利用哈希函数 $h(x)$ 生成证书的新版本号 $v_{a-ver+1} = h(v_{a-ver})$, 相应的新证书表示为 $CERT_{a-ver+1}$, 新假名表示为 $PID_{a-ver+1}$;

② TA_x 将 v_{a-ver} 放在第 m 个哈希桶的第 n 个位置中, 记为 $(m, n)_{a-ver}$, 哈希桶中版本号与吊销证书表 CRL 一一映射;

③ TA_x 以增量方式周期性的更新 OBU_a 中证书吊销列表 CRL;

④ 若某一哈希桶满, 启用备用哈希桶。

3.4.2 证书吊销消息及更新报文的发布

证书吊销消息及更新报文发布的步骤:

① TA_x 随机选择 $d \in Z_q^*$ (Z_q^* 为有理数集), 当证书版本号为 $v_{a-ver+1}$ 时, TA_x 选择 OBU_a 的新公钥 $PK_{a-ver+1} = P/k_{a-ver+1} \in U_{xp}$, 新私钥 $SK_{a-ver+1} = f(SK_{a-ver}, PK_{a-ver+1}) \in U_{xs}$, 其中 $f(SK_{a-ver}, PK_{a-ver+1})$ 为 OBU_a 事先与 TA_x 约定的新私钥的生成规则。

② TA_x 计算中间键。

$PK_{ma} = dPK_{a-ver+1} = dP/k_{a-ver+1}$ 。

③ TA_x 计算出自己的新密钥 $K_{ga-ver+1}$ 供 TA_x 范围内的 OBU 共享

$$\begin{aligned} K_{ga-ver+1} &= \hat{e}(SK_{a-ver+1}, PK_{ma}) \\ &= \hat{e}(k_{a-ver+1}Q, dP/k_{a-ver+1}) \\ &= \hat{e}(Q, P)^{k_{a-ver+1} \cdot d/k_{a-ver+1}} \\ &= \hat{e}(Q, P)^d \end{aligned}$$

④ 计算吊销通知 REV_{msg-a}

$REV_{msg-a} = HMAC(v_{a-ver} || K_{ga-ver+1} || m)$ 。

⑤ TA_x 使用 $K_{ga-ver+1}$ 对版本号 $v_{a-ver+1}$ 对称加密得到 $ENC_{ga-ver+1}(v_{a-ver+1} || T_{stamp-ver+1})$, 其中 $v_{a-ver+1}$ 是新证书版本号。

⑥ 生成 TA_x 签名及更新报文 $M_{a-ver+1}$

$sig_{TA_x}(PID_{a-ver+1} || PK_{a-ver+1})$

$M_{a-ver+1} = (MK^+, sig_{TA_x}(PID_{a-ver+1} || PK_{a-ver+1}) || ENC_{ga-ver+1}(v_{a-ver+1} || T_{stamp-ver+1}))$ 。

其中 MK^+ 是 MA 的公钥。

⑦ TA_x 发布吊销消息 REV_{msg-a} 及更新报文 $M_{a-ver+1}$ 。

3.5 OBU_b 对吊销消息的处理

OBU_b 计算 REV_{msg-a} , 与收到的吊销通知

REV_{msg-a} 相比较,若相等则丢弃消息 m , 否则接受 m .

3.6 OBU_a 对更新报文 $M_{a-ver+1}$ 的处理

OBU_a 对更新报文 $M_{a-ver+1}$ 的处理步骤:

① OBU_a 利用新共享密钥 $K_{ga-ver+1}$ 解出 $M_{a-ver+1}$ 中的版本号 $v_{a-ver+1}$, 时间戳 $T_{stamp-ver+1}$ 及 $sig_{TA_x}(PID_{a-ver+1} || PK_{a-ver+1})$ 中 OBU_a 的新假名 $PID_{a-ver+1}$ 和新公钥 $PK_{a-ver+1}$.

② OBU_a 更新证书版本号及假名分别为 $v_{a-ver+1}$ 和 $PID_{a-ver+1}$, OBU_a 根据先前与 TA_x 约定的密钥变化规则更新自己的私钥 $SK_{a-ver+1}$.

4 安全性分析

(1) 数据源不可伪造

OBU 发送的消息中包括自己的签名、TA 的签名、目的节点的公钥等,可以提高安全强度,且椭圆曲线双线性对的 2 个 NP 问题(双线性的判定性和计算性问题)确保了倍点运算的不可逆性,使攻击者无法通过捕获的认证信息推算出车辆节点或 RSU 的身份信息和签名证书,有效地防止了攻击者利用伪造证书进行攻击.

(2) 匿名性

由于 OBU 的真实身份已经在注册时通过加密转换成假名,保证了匿名性和不可关联性,达到隐私保护的目.

(3) OBU 可追查性

当发生事故或者安全消息存在争议时,TA 在协助 MA 打开签名,证明签名者确实签署过这个签名.

(4) 前向安全性

由于安全的哈希函数具有单向的加密属性,是不可逆的,攻击者不可以从当前哈希链的值 $v_{a-ver+1}$ 得到前驱哈希值 v_{a-ver} , 因此前向安全性得到保证.

5 性能分析

5.1 吊销检查的复杂性分析

用 N_{rev} 表示 CRL 中吊销证书的总数. 线性搜索算法需要对 CRL 进行全表扫描,且逐一比较,计算复杂度是 $O(N_{rev})$. 二进制搜索算法类似折半查找,计算复杂度是 $O(\log(N_{check}))^{[8]}$. CPMA 只需将所计算的 REV_{msg-a} 值和接收的 REV_{msg-a} 值进行比较即可. 与线性和二进制搜索算法相比,CPMA 的计算复杂度最低.

5.2 认证延迟分析

为了验证 CPMA 方法的有效性,作者在英特尔酷睿 2 GHz 的机器上使用 C++ 编程模拟了 CPMA、线性及二进制 CRL 检查的过程. 可以看出:① 线性 CRL 的认证延迟随被吊销证书数量的增加而增加;② 二进制 CRL 的认证延迟基本稳定;③ CPMA 的认证延迟最稳定,与吊销证书的数量基本无关. CPMA 在相同的时间内可以验证更多的消息.

5.3 消息丢失率分析

根据专用短程通信标准(DSRC),每个 OBU 每隔 300 ms 广播发送其位置、速度和其他路况信息. 在 20 000 个证书的情况下分别进行线性搜索算法,二进制搜索算法和 CPMA 搜索算法的模拟实验,在 300 ms 内平均每个 OBU 的消息丢失率如图 4 所示.

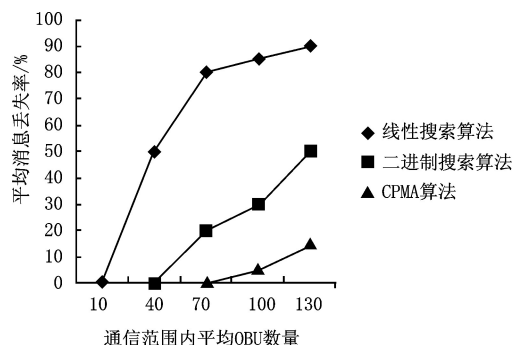


图4 平均消息丢失率与平均 OBU 数量的关系

与线性搜索算法和二进制搜索算法相比,在通信范围内 OBU 数量一定时 CPMA 消息丢失率较小.

由于本方案增加了假名、共享密钥等信息,会增加一些额外的存储开销.

6 结束语

本文提出的条件隐私保护方法,使用密钥共享机制,允许动态更新 OBU 证书与密钥,采用基于 Hash 消息认证码的分级 CRL 检查方法优化了证书的有效性检查过程,在保证安全性的同时能有效降低证书的认证延迟. 分布式认证方法是下一步研究的重点.

参考文献:

- [1] 常促宇,向勇,史美林. 车载自组织网的现状与发展[J]. 通信学报,2007,28(11):116-124.

(下转第 102 页)

参考文献:

- [1] 朱颜锐,田斌,安金坤,等. 一种快速 OFDM 调制信号识别算法[J]. 西安电子科技大学学报:自然科学版, 2012,39(1):17-22.
- [2] 王晓东,刘镝. 一种 MPSK 信号调制方式[J]. 电声技术, 2013,37(2):74-83.
- [3] 王永娟,基于高阶累积量的 OFDM 信号调制识别技术研究[D]. 西安:西安电子科技大学,2009.
- [4] AKMOUCHEW. Detection of multicarrier modulations using 4th-order cumulants [C]//MILCOM'99, Atlantic City, NJ:IEEE, 1999: 432-436.
- [5] 刘献玲,陈健,阔永红,等. 基于累量的 OFDM 信号调制识别[J]. 电子科技, 2007,209(2):29-32.
- [6] 郭黎明,于志明. 基于多参数特征的 OFDM 信号盲识别[J]. 西南交通大学学报, 2010,45(5):732-738.
- [7] 李彦栓,罗明,李霞. 基于高阶累积量的 OFDM 信号调制识别技术[J]. 电子信息对抗技术, 2012,27(4):1-4.
- [8] Chan Y, Gadbois L. Identification of the modulation type of a signal[J]. Signal Processing, 1989, 16(2): 149-154.
- [9] 周敏. 数字通信信号制式自动识别与参数估计算法研究与实现[D]. 成都:西南交通大学,2013.
- [10] Lan-Xun W, Yu-Jing R. Recognition of digital modulation signals based on high order cumulants and support

vector machines[C]//CCCM 2009, ISECS International Colloquium on. [s. l.]:IEEE, 2009:271-274.

- [11] 黄如容. 数字信号调制方式识别方法的设计与实现[D]. 成都:西南交通大学,2012.
- [12] 徐勋华,王继成. 支撑向量机的多类分类方法[J]. 微电子学与计算机, 2004,21(10):149-152.

作者简介:



史文娟 女, (1990-), 硕士研究生. 研究方向为数字信号处理.



冯全源 男, (1963-), 博士生导师, IEEE 高级会员. 研究方向为数字、模拟、射频与混合信号集成电路设计, 数字系统设计和嵌入式系统研究, 现代天线技术、RFID 技术(物联网技术).

(上接第 97 页)

- [2] 张建明,杨玉娟,江浩斌,等. 车辆自组网的位置隐私保护技术研究[J]. 通信学报, 2012, 33(8): 180-189.
- [3] Xiong Hu, Zhiguang Qin, Fagen Li, et al. Secure vehicle-to-roadside communication protocol using certificate-based crypto system[J]. IETE Technical Review, 2010, 27(3): 214-219.
- [4] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, et al. GSIS: a secure and privacy preserving protocol for vehicular communications[J]. IEEE Trans on Vehicular Technology, 2007, 56(6): 3442-3456.
- [5] N Koblitz, A Menezes, S Vanstone, et al. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2): 173-193
- [6] Morten Dahl, Stephanie Delaune. Formal analysis of Privacy for vehicular mix-zones[C]// Proceedings of the 15th European Symposium on Research in Comput-

er Security, 2010: 55-70.

- [7] Albert Wasef, Yixin Jiang, Chuang Lin, et al. DCS: an efficient distributed certificate service scheme for vehicular networks[J]. IEEE Trans. on Vehicular Technology, 2010, 59(2): 533-549.
- [8] Johnson Don, Menezes Alfred, Vanstone Scott, et al. The elliptic curve digital signature algorithm (ECDSA) [J]. Int'l J. Information Security, 2001, 1(1): 36-63.

作者简介:

张盼盼 女, (1985-), 硕士研究生. 研究领域为网络安全技术.

沈明玉 男, (1962-), 博士, 副教授, 硕士生导师. 研究方向为网络与信息安全.