

基于强化学习的低时延车联网群密钥分配管理技术

徐堂炜¹, 张海璐¹, 刘楚环¹, 肖亮¹, 朱珍民²

(1. 厦门大学信息学院, 福建 厦门 361005;

2. 中国科学院大学计算技术研究所, 北京 100190)

摘要: 车联网的通信密钥管理水平决定其信息保密性和抵御电子欺骗等基于用户身份的攻击的安全性。现有密钥管理方案采用固定频率更新车联网的群密钥, 增大了密钥更新时延和加密时延。提出一种基于强化学习的低时延车联网群密钥分配管理技术, 令群首车辆根据周边车辆数目变化和密钥更新记录等因素优化其群密钥的更新频率和密钥长度。该技术不需要群首车辆预知附近的车流变化模型与访问驱动高速缓存攻击模型, 降低加解密时延, 并在基于高级加密标准的车联网仿真进行验证。仿真结果表明, 相比基准的群密钥管理方案, 该技术降低密钥更新的传输时延, 减少车联网的加解密计算时延, 并提高群密钥的保密性。

关键词: 车联网; 密钥管理; 强化学习

中图分类号: TN97

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020055

Reinforcement learning based group key agreement scheme with reduced latency for VANET

XU Tangwei¹, ZHANG Hailu¹, LIU Chuhuan¹, XIAO Liang¹, ZHU Zhenmin²

1. School of Informatics, Xiamen University, Xiamen 361005, China

2. Institute of Computing technology, Chinese Academy of Sciences University, Beijing 100190, China

Abstract: Key agreement scheme of vehicle ad hoc networks (VANET) determines the privacy and security against user identity-based attacks, such as spoofing attack. The existing work updates the group shared key at a fixed frequency, which increases the processing latency of the key updates and the encryption and decryption of group communication. A reinforcement learning based dynamic key agreement scheme was proposed to enable the group cluster head to optimize the key update frequency and key length. This scheme optimizes the calculation latency of encryption and decryption based on the number of surrounding vehicles, the previous key update records without the knowledge of the traffic flow model and the access-driven cache attack model. Simulation results show that this

收稿日期: 2020-01-16; 修回日期: 2020-03-19

通信作者: 肖亮, lxiao@xmu.edu.cn

基金项目: 国家自然科学基金 (61971366)

Foundation Item: The National Natural Science Foundation of China (61971366)

论文引用格式: 徐堂炜, 张海璐, 刘楚环, 等. 基于强化学习的低时延车联网群密钥分配管理技术[J]. 网络与信息安全学报, 2020, 6(5): 119-125.

XU T W, ZHANG H L, LIU C H, et al. Reinforcement learning based group key agreement scheme with reduced latency for VANET[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 119-125.

scheme reduces the transmission delay of the communication overhead and the computational latency of encryption and decryption, and improves the security of the group key compared with the benchmark scheme.

Key words: VANET, group key agreement, reinforcement learning

1 引言

车联网(VANET, vehicular Ad Hoc networks)群集内共享群密钥对群成员通信进行对称加密^[1],是保障群集车辆协同驾驶、拥塞避免以及娱乐服务过程中通信安全和用户隐私的关键^[2-3]。由于车联网群集的动态性和开放性,群集容易遭受各种内外部网络攻击,攻击者利用时序攻击、缓存攻击^[4]等手段窃取群密钥,进行窃听、电子欺骗等攻击,导致用户隐私泄露与交通事故。因此,车联网需要实时更新群密钥,保障群密钥在车辆加入和离开群集的前向安全和后向安全^[5]。

车联网群集使用群密钥对车辆进行节点认证和通信加密受到广泛关注的同时,如何有效管理车联网密钥是一个亟须解决的问题。文献[6]提出基于公钥基础设施(PKI, public key infrastructure)的车联网匿名密钥管理方案,通过匿名数字证书认证车辆节点和保护数据完整性,但随着车辆节点数的增加,大量的密钥和匿名证书使认证中心需付出较大的管理成本以确保系统安全,并对车辆节点的存储和通信开销带来负担。文献[7]提出使用基于群集的对等批密钥协议,但车辆节点只能属于一个群集,且当新节点加入群集时,群首需要重新与群成员逐个协商密钥,难以适用于高动态性的车联网。Islam等^[8]提出的GKA方案使用假名对群集进行认证与密钥更新,通过假名构建数字签名的同时对群集车辆进行认证,防止车辆轨迹隐私的泄露。文献[5]提出使用软件定义网络对车联网进行管理,不同群集自主构建去中心化网络进行通信,同时使用中心网络对群集进行认证与密钥管理。针对群集去中心化网络, Jiang等^[9]提出通过计算哈希消息认证码取代认证撤销列表对车辆进行分布式批量匿名认证,该方案保护用户隐私的同时,减小认证时延; Liu等^[10]提出在信任机制基础上,信誉度高的车辆通过信任中心认证后,可进行匿名密钥协商,在保护隐私的同时,确保消息机密性和完整性。

强化学习作为机器学习的主要研究方向,被

广泛用于车联网通信安全^[11-12]。Xiao等^[13-14]提出使用强化学习辅助移动设备优化中继方案、发射功率和通信频点等以抵抗敌意干扰,该方案在降低能耗的同时,保证了通信可靠性。文献[15-16]在未知信道模型与电子欺骗攻击模型的情况下,使用强化学习优化接收信号强度等无线信道物理层特征的认证阈值,在恶意发送者的动态博弈中实现高精度认证。Chu等^[17]使用基于长短期记忆效应的强化学习进行用户联合接入控制和电池能量预测,在提升网络吞吐量的同时,节约能耗。文献[18]提出使用强化学习根据当前缓存使用状况和信道状态进行联合缓存分配和干扰对齐,以解决无线通信中的多用户干扰,提升传输速率。

本文立足于车联网群集内通信安全,以群集群密钥分配管理为研究对象。在该网络中,同一区域具有共同利益的车辆(如目的地、爱好、朋友圈等)构建群集,协作形成基于车辆队列的驾驶模式,分享路况及驾驶信息,以很小且恒定的车距提高道路通行能力和能源效率,并提供多媒体服务。由于车辆频繁加入和离开群集,为保证群集内车辆通行安全,防止电子欺骗等攻击,对路况、多媒体等部分群集内信息进行加密,且需要实时更新群密钥。与传统PKI相比,本文提出一种无证书签名方案,该方案摒弃了数字证书的使用,通过信任中心与车辆间保密存储的随机质数对群密钥签名,确保数据完整性,并借助路边单元(RSU, road side unit)广播群密钥更新信息,实现群密钥同步更新,减少车辆节点更新群密钥的通信开销,降低群密钥更新传输时延。群首在群密钥更新策略无前效性的情况下,群密钥的更新策略仅与群集当前状态有关,因而将密钥更新策略的优化过程构建为马尔可夫决策过程。为了得到动态群集环境中最优的密钥更新频率与密钥长度,本文提出了基于强化学习的低时延群密钥分配管理技术,在未知群集的车流变化模型和访问驱动高速缓存攻击模型的前提下,该技术根据群集车辆数目、群集车辆数目变化、之前时段密

钥更新决策和当前群集通信的安全等级，使用强化学习优化群密钥的更新频率和密钥长度，在不断试错与借鉴的学习中，获得最优密钥更新策略，降低群集通信加解密的计算时延和群密钥被窃取的概率，提升群集通信服务质量。

2 系统模型

2.1 密钥管理模型

车联网低时延密钥管理技术主要由装配于车辆的车载单元（OBU，on board unit）、路边单元和信任机构（TA，trusted authority）组成。OBU 以专用短距离通信（DSRC，dedicated short range communication）协议^[19]为基础与 RSU 和周围车辆通信。RSU 作为一个通信中继与广播节点，通过有线网络和 TA 连接，并与 OBU 通过无线网络通信。当所有车辆首次进入 TA 注册时，TA 分发车辆身份标识 ID，产生随机质数 n 用于生成群密钥与加密群密钥，产生公钥 VPK 和私钥 VSK，登记 $\{ID, n, VPK\}$ ，并将 $\{ID, n, VSK\}$ 存放在车辆的 OBU 中。TA 登记 RSU 的身份标识 RID 和其公钥 RPK，并将其私钥 RSK 存储于 RSU。

表 1 重要参数符号
Table 1 Notations of important parameters

参数	含义
M^k	k 时刻群集内车辆数目
v^k	群集车辆平均速度
g^k	前 D 个时刻群集密钥更新决策
ρ^k	群集通信安全等级
x_1^k	更新密钥决策
x_2^k	更新密钥长度
λ	泊松分布均值
VPK/VSK	车辆的公钥/私钥
RPK/RSK	RSU 的公钥/私钥
n	TA 选择的随机质数
$E(\cdot)$	加密
$h(\cdot)$	Hash 函数
T/T^*	发送/接收时间戳

如图 1 所示，车联网基于动态聚类算法在一定区域内组织 M 个车辆节点 $\{Veh_i\}_{1 \leq i \leq M}$ 构建群集^[20]，并为其提供协同驾驶、拥塞避免等服务；

由于高速行驶的车辆加入和离开群集具有一定随机性，因而需要实时更新群密钥。假设单位时间内加入和离开群集的车辆节点数服从均值为 λ 的泊松分布，群集车辆身份标识为 $\{ID_i\}_{1 \leq i \leq M}$ 。为了保证群集内的通信和隐私安全，群集内通信采用对称加密机制，并采用无证书签名密钥管理方案更新群密钥。群首（cluster head） Veh_F 为群集生成密钥更新请求，RSU 负责将该请求进行二次加密并转发给 TA，TA 根据请求反馈新密钥。具体而言，群首 Veh_F 观察群集内车辆的数目，加入和离开群集的车辆数目，群集的平均行驶速度，前 D 个时刻的密钥更新决策和当前时刻的安全等级，生成密钥更新请求。密钥更新请求主要包含更新密钥的群集车辆 ID 和新密钥的长度 x_2 ，即 $x_2 \parallel \{ID_i\}_{1 \leq i \leq M}$ 。 Veh_F 使用私钥 VSK_F 加密密钥更新请求，添加时间戳 T_1 发送给 RSU。RSU 于 T_1^* 收到密钥更新请求后，计算 $T_1^* - T_1$ ，用于验证密钥更新请求的有效性，防止重放攻击。若 $T_1^* - T_1 < \Delta T_1$ ，RSU 使用私钥 RSK 再次加密密钥更新请求，通过有线网络将密钥更新请求发送给 TA。

TA 接收到 RSU 转发的密钥更新请求，首先计算 $T_2^* - T_2 < \Delta T_2$ ，验证密钥更新请求的有效性。TA 使用公钥 RPK 和 VPK_F 解密密钥更新请求，实现对 Veh_F 和 RSU 进行认证的同时，获得新密钥长度 x_2 和身份标识 $\{ID_i\}_{1 \leq i \leq M}$ 。TA 根据 $\{ID_i\}_{1 \leq i \leq M}$ 对应的 $\{n_i\}_{1 \leq i \leq M}$ ，使用基于中国剩余定理的 HCPA-GKA^[21] 算法，生成长度为 x_2 的群密钥 ψ ，并计算哈希值 $h(\psi)$ 生成数字签名。TA 使用 $\{n_i\}_{1 \leq i \leq M}$ 与 ψ 进行异或运算加密群密钥，并采用 $\{VPK_i\}_{1 \leq i \leq M}$ 对异或结果进行加密保证密钥传输安全，即生成 $h(\psi) \parallel \{E_{VPK_i}(\psi \oplus n_i)\}_{1 \leq i \leq M}$ 。TA 将 $ID_F \parallel h(\psi) \parallel \{E_{VPK_i}(\psi \oplus n_i)\}_{1 \leq i \leq M}$ 使用 RPK 进行加密后发送给 RSU，RSU 将其解密后广播给群集车辆 $\{Veh_i\}_{1 \leq i \leq M}$ 。

群成员 Veh_i 接收 RSU 广播的密钥更新消息，使用私钥 VSK_i 解密 ID_i 对应的 $E_{VPK_i}(\psi \oplus n_i)$ 部分，获得 $\psi \oplus n_i$ 。群成员使用 OBU 中存储的随机质数 n_i 解密 $\psi^* = \psi \oplus n_i \oplus n_i$ 获得群密钥 ψ^* ，并计算其 hash 值 $h(\psi^*)$ 校验新密钥 ψ^* 的真实性。

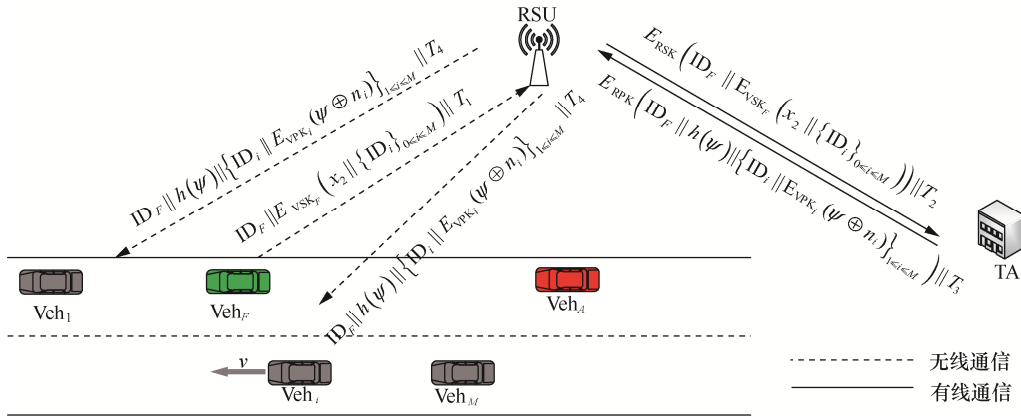


图 1 密钥管理模型
Figure 1 Key agreement model

若 $h(\psi^*) \neq h(\psi)$ ，接收到的密钥更新信息为伪造消息；否则，更新 ψ^* 作为群集内通信的新密钥。

2.2 攻击模型

本文主要考虑车联网内部攻击，攻击者可以是网络内部合法的车辆节点，或者被控制的恶意车辆节点，其通过时序攻击、缓存攻击^[4]等边信道攻击手段获取群密钥，进而实施电子欺骗攻击^[8]等。具体而言，攻击者使用间谍程序观察加密过程中的时延边信道信息，监视缓存的命中与未命中，从而窃取加密密钥。攻击者冒充已经获得身份验证的车辆或 RSU，通过合法身份将恶意信息或伪造的信息，如车流密度信息、碰撞避免信息，发送给周围车辆，甚至冒充合法身份的车辆将该车辆从 VANET 中移除。假设每个车辆节点发动内部攻击成功的概率为 y ，拥有车辆数目 M 的群集被攻击的概率为 $1 - (1 - y)^M$ 。其中，群集被攻击成功的概率与群集车辆数目和密钥更新频率呈正相关，与密钥长度呈负相关。

3 基于强化学习的密钥管理技术

随着车辆的加入、离开，群集的合并、拆分和通信安全等级的变化，群首需要实时更新群集内通信的群密钥。群密钥的密钥长度和更新频率与群集通信安全等级、通信加密与解密计算时延的动态优化过程可以视为一个马尔可夫过程。本文提出一种基于强化学习的低时延车联网群密钥分配管理技术，群首优化群密钥的长度和更新频率，通过不断试错与学习，获得最优的密钥更新

策略。

在该技术中，群集基于物理层特征，如信道状态和接收信号强度等，进行入侵检测^[22]， Veh_F 根据反馈的检测结果评估群集的通信安全等级 ρ 。当群集检测到车辆遭受电子欺骗等攻击时， $\rho = 0$ ；否则， $\rho = 1$ 。群首 Veh_F 综合考虑群集的车辆数目 M ，群集平均速度 v ，前 D 个时刻内密钥更新决策 $\mathbf{g}$ 和上一时刻群集通信的安全等级 ρ 等信息，根据群集的长期学习效益，选择密钥更新策略 $\mathbf{x} \in \mathcal{A}$ ，包含是否发送密钥更新请求 $x_1 \in \{0, 1\}$ 与更新的密钥长度 $x_2 \in [1, L_A]$ bit，即 $\mathbf{x} = [x_1, x_2]$ 。其中， L_A 为密钥长度的上限值， $\mathcal{A}$ 为密钥管理动作空间。当 $x_1 = 0$ 时， Veh_F 不发送密钥更新请求，群集继续使用之前的密钥进行通信加密；当 $x_1 = 1$ 时， Veh_F 向 TA 请求更新长度为 x_2 的群密钥。

在 k 时刻， Veh_F 观察群集内 $k-1$ 时刻和 k 时刻的车辆数目 M^{k-1} 和 M^k ，群集车辆平均行驶速度 v^k ，前 D 个时刻密钥更新决策 $\mathbf{g}^k = [x_1^i]_{k-D \leq i \leq k-1}$ 和 $k-1$ 时刻群集通信的安全等级 ρ^{k-1} ，构建当前群集状态 $\mathbf{s}^k$ 。

$$\mathbf{s}^k = [M^{k-1}, M^k, v^k, \mathbf{g}^k, \rho^{k-1}] \quad (1)$$

令 $Q(\mathbf{s}, \mathbf{x})$ 表示 Veh_F 在 $\mathbf{s}$ 状态下采取行动 $\mathbf{x}$ 的长期收益， Veh_F 根据当前群集的状态 $\mathbf{s}^k$ ，通过对应的 Q 值采用 ε -贪婪策略选择群密钥的更新策略 $\mathbf{x}^k = [x_1^k, x_2^k]$ 。具体而言， Veh_F 以 $1 - \varepsilon$ 的

概率选择当前状态 s^k 中长期收益 $Q(s^k, x)$ 最大的密钥更新策略；以 ε 的概率从 A 中任意选择一个密钥更新策略，即

$$p(x^k = x^*) = \begin{cases} 1 - \varepsilon, & x^* = \arg \max_{x \in A} Q(s^k, x) \\ \frac{\varepsilon}{|A|}, & \forall x^* \in A \end{cases} \quad (2)$$

在 k 时刻，若 Veh_F 向 TA 发送经由 RSU 转发的密钥更新请求，该请求包含群集车辆身份标识 $\{ID_i\}_{1 \leq i \leq M}$ 和密钥长度 x_2^k ；TA 接收密钥更新请求并生成群密钥 ψ 返回给 RSU；RSU 接收到被加密的新密钥后，将其广播给群集车辆以实现对整个群集密钥的更新。

当群集进行密钥更新后， Veh_F 通过群集成员的反馈获得当前群集内通信的安全等级 ρ^k ，并评估群集加密与解密长度为 x_2^k 的群密钥的计算时延。 Veh_F 通过群集车辆数目 M^k 、群集通信安全等级 ρ^k 和密钥长度 x_2^k 评估此次密钥更新的收益 u^k 。

$$u^k = \rho^k M^k - c_1 x_2^k M^k - c_2 x_1^k M^k \quad (3)$$

其中， c_1 和 c_2 分别表示群集通信加密与解密的计算时延和密钥更新时延的权重。

Veh_F 观察群集 $k+1$ 时刻状态 s^{k+1} ，基于贝尔曼方程，更新状态动作对 (s^k, x^k) 对应的 Q 值，即

$$Q(s^k, x^k) \leftarrow (1 - \alpha) Q(s^k, x^k) + \beta \left(u^k + \max_{x \in A} Q(s^{k+1}, x^k) \right) \quad (4)$$

基于强化学习的车联网密钥管理技术的具体过程如算法 1 所示。

算法 1 基于强化学习的低时延车联网密钥分配管理算法

- 1) 初始化 α , β , $Q=0$, s^1 , $k=1$, K 。
- 2) 观测 $k-1$ 时刻和 k 时刻车辆数目 M^{k-1} 与 M^k ，车速 v^k ，前 D 个时刻内密钥更新情况 g^k 和 $k-1$ 时刻通信安全等级 ρ^{k-1} 。
- 3) 构建当前 k 时刻群集的状态 $s^k = [M^{k-1}, M^k, v^k, g^k, \rho^{k-1}]$ 。

4) 根据式(2)选择密钥更新策略 $x^k = [x_1^k, x_2^k]$ 。

5) 当 $x_1^k = 1$ 时，执行以下操作：

① 请求 TA 生成长度为 x_2^k 的群密钥 ψ ；②

RSU 将密钥更新消息广播给群集车辆 $\{Veh_i\}_{1 \leq i \leq M^k}$ 。

6) 评估当前通信安全等级 ρ^k 。

7) 根据式(3)获取效益 u^k 。

8) 根据式(4)更新 $Q(s^k, x^k)$ 。

9) 若 $k = K$ ，则结束学习；否则， $k = k+1$ ，跳转至步骤 2)。

4 仿真实验

为了验证基于强化学习的低时延车联网群密钥分配管理技术在加密与解密的计算时延和通信安全等级上的优势，本文利用 Python 构建动态群集仿真场景。仿真参数设置参考文献[23]，具体如下：群首与 300 m 范围内的车辆构成群集，起始群集车辆节点数目为 50，群集内车辆平均速度 $v \in [0, 120]$ km/h 且与群集车辆数目呈反比^[24]。群集车辆使用高级加密标准 (AES, advanced encryption standard) 对称加密算法对群集内通信进行加密，可选密钥长度 $x_2 \in \{128, 192, 256\}$ bit。群集内车辆通信的数据包大小为 1 kB。Q 学习的学习率 $\alpha=0.2$ ，折扣因子 $\beta=0.8$ 。

图 2 提供了 3 000 个时隙内基于强化学习的密钥管理技术 (RLKA) 的平均性能，考察了单位时隙加入和离开群集的平均车辆数目 $\lambda \in \{1, 2, \dots, 5\}$ 对加密与解密计算时延和群集通信安全等级的影响。当 λ 从 1 增加到 5 时，群集内车辆加密和解密 1 kB 数据包的计算时延从 432 μ s 增加至 497 μ s，时延增大了 15.0%；群集通信安全等级从 0.963 降低至 0.794，性能降低了 17.5%。当 $\lambda=3$ 时，与 GKA 方案相比，本文所提技术的加解密计算时延降低了 18.1%，安全等级提升 24.1%。这是因为与 GKA 方案固定的密钥长度和更新频率相比，本文提出的 RLKA 技术能够根据当前群集的车辆数目、车辆加入与离开群集数目和群集车辆入侵检测安全反馈等车联网相关信息，通过合理地更新密钥与控制密钥长度，降低

恶意节点攻击成功概率, 保证车联网群集通信安全并获得更小的加解密计算时延开销。

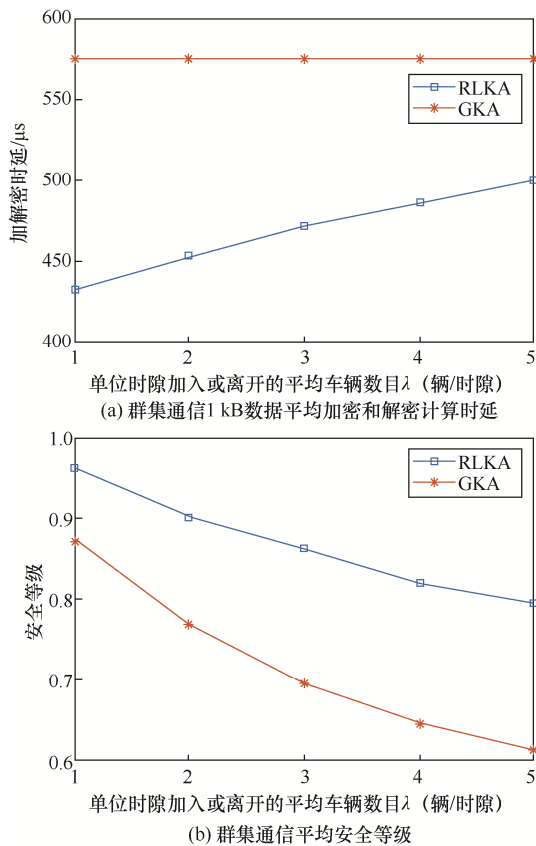


图2 车联网密钥管理平均性能

Figure 2 Average performance of key agreement in VANET

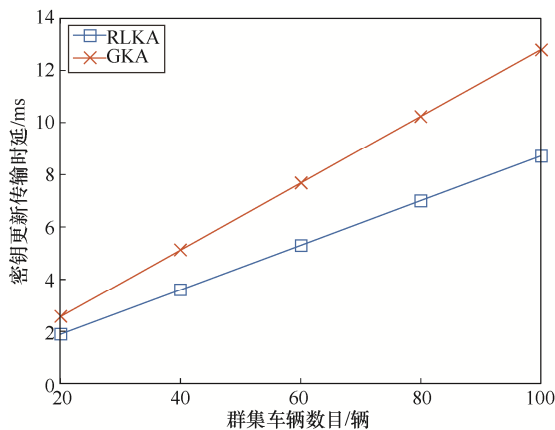


图3 密钥更新传输时延

Figure 3 The transmission delay of key update

为了验证使用无证书签名的 RLKA 技术在通信开销上的优势, 本文利用 Matlab 构建密钥更新传输时延的仿真。仿真参数设置参考文献[9], 车辆节点与 RSU 间的无线传输速率为 600 Mbit/s,

车辆 ID、时间戳 T 、请求密钥长度 x_2 的数据大小为 4 byte。如图 3 所示, 当群集车辆数目从 20 辆增加到 100 辆时, 由于密钥更新信息的数据量增大, 群集密钥更新信息的传输时延随群集车辆数目线性增加。当群集车辆数为 60 时, 与 GKA^[8]方案相比, 本文所提技术的密钥更新传输时延降低了 31.0%。相比基于 PKI 的车联网密钥管理方案, 本文使用无证书签名密钥管理技术, 摒弃了数字证书, 避免传输数字证书带来的通信时延和通信负载, 并通过 RSU 广播实现群密钥的快速同步更新。

5 结束语

本文提出了一种基于强化学习的低时延车联网群密钥分配管理技术, 群首车辆观测周围车辆变化数目、车辆行驶速度等群集特征, 结合之前时刻密钥更新决策与当前车联网通信安全情况构建群集状态, 使用强化学习优化群密钥的更新频率和密钥长度, 通过低时延群集密钥更新实现对密钥窃取和电子欺骗等攻击的抵抗, 提升群集通信安全等级, 降低群集内通信时延。仿真结果表明, 与 GKA^[8]方案相比, 本文提出的 RLKA 技术保证通信安全的同时, 降低群密钥更新传输时延, 减小群集内通信加密与解密的计算时延, 提高群密钥保密性, 提升群集通信服务质量。

参考文献:

- [1] 刘俊杰, 赵佳, 张强, 等. 军事车联网密钥管理方案研究[J]. 网络与信息安全学报, 2018, 4(8): 39-46.
LIU J J, ZHAO J, ZHANG Q, et al. Research on key management scheme for military vehicle network[J]. Chinese Journal of Network and Information Security, 2018, 4(8): 39-46.
- [2] LU Z J, QU G, LIU Z L. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(2): 760-776.
- [3] 王良民, 李婷婷. 基于车辆身份的车联网结构与安全[J]. 网络与信息安全学报, 2016, 2(2): 41-54.
WANG L M, LI T T. Structure and security of vehicle network based on vehicle identity[J]. Chinese Journal of Network and Information Security, 2016, 2(2): 41-54.
- [4] GULLASCH D, BANGERTER E, KRENN S. Cache games-bringing access-based cache attacks on AES to practice[C]//IEEE Symposium on Security and Privacy. 2011: 490-505.
- [5] LAI C Z, ZHOU H B, CHENG N, et al. Secure group communications in vehicular networks: a software-defined network-enabled architecture and solution[J]. IEEE Vehicular Technology Magazine, 2017, 12(4): 40-49.
- [6] RAYA M, HUBAUX J P. Securing vehicular Ad Hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.

- [7] YEHL Y, HUANG Y L, JOSEPH A D, et al. A batch-authenticated and key agreement framework for P2P-based online social networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1907-1924.
- [8] ISLAM S K H, OBAIDAT M S, VIJAYAKUMAR P, et al. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs[J]. Future Generation Computer Systems, 2018, 84(7): 216-227.
- [9] JIANG S R, ZHU X Y, WANG L M. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.
- [10] LIU Y B, WANG Y H, CHANG G H. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(10): 2740-2749.
- [11] XIAO L, ZHUANG W H, ZHOU S, et al. Learning-based VANET communication and security techniques[M]. Berlin: Springer, 2019.
- [12] LUONG N C, HOANG D T, GONG S, et al. Applications of deep reinforcement learning in communications and networking: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3133-3174.
- [13] XIAO L, LU X Z, XU D J, et al. UAV relay in VANETs against smart jamming with reinforcement learning[J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4087-4097.
- [14] XIAO L, JIANG D H, XU D J, et al. Two-dimensional anti-jamming mobile communication based on reinforcement learning[J]. IEEE Transactions on Vehicular Technology, 2018, 67(10): 9499-9512.
- [15] XIAO L, WAN X Y, HAN Z. PHY-layer authentication with multiple landmarks with reduced overhead[J]. IEEE Transactions on Wireless Communications, 2017, 17(3): 1676-1687.
- [16] XIAO L, CHEN T H, HAN G A, et al. Game theoretic study on channel-based authentication in MIMO systems[J]. IEEE Transactions on Vehicular Technology, 2017, 66(8): 7474-7484.
- [17] CHU M, LI H, LIAO X W, et al. Reinforcement learning-based multiaccess control and battery prediction with energy harvesting in IoT systems[J]. IEEE Internet of Things Journal, 2018, 6(2): 2009-2020.
- [18] HE Y, ZHANG Z, YU F R, et al. Deep-reinforcement learning based optimization for cache enabled opportunistic interference alignment wireless networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 10433-10445.
- [19] JIANG D, TALIWAL V, MEIER A, et al. Design of 5.9 GHz DSRC-based vehicular safety communication[J]. IEEE Wireless Communications, 2006, 13(5): 36-43.
- [20] REN M, KHOUKHI L, LABIOD H, et al. A mobility-based scheme for dynamic clustering in vehicular Ad-Hoc networks (VANETs)[J]. Vehicular Communications, 2017, 9(3): 233-241.
- [21] CUI J, TAO X, ZHANG J, et al. HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs[J]. Vehicular Communications, 2018, 14(3): 15-25.
- [22] XIAO L, LI Y, HAN G, et al. PHY-layer spoofing detection with reinforcement learning in wireless networks[J]. IEEE Transactions on Vehicular Technology, 2016, 65(12): 10037-10047.
- [23] CHEN C, XIAO T T, ZHAO H H, et al. GAS: a group acknowledgment strategy for popular content distribution in Internet of vehicle[J]. Vehicular Communications, 2019, 17(3): 35-49.
- [24] ZAIDI K, MILOJEVIC M B, RAKOCEVIC V, et al. Host-based intrusion detection for VANETs: a statistical approach to rogue node detection[J]. IEEE Transactions on Vehicular Technology, 2015, 65(8): 6703-6714.

[作者简介]



徐堂炜（1995—），男，福建三明人，厦门大学硕士生，主要研究方向为车联网、强化学习。



张海璐（1996—），女，福建龙岩人，厦门大学硕士生，主要研究方向为无线通信、网络安全。



刘楚环（1993—），男，安徽宿州人，厦门大学博士生，主要研究方向为无线通信、车联网网络安全。



肖亮（1980—），女，河北石家庄人，厦门大学教授、博士生导师，主要研究方向为网络安全、通信与网络。



朱珍民（1962—），男，湖南慈利人，中国科学院大学教授，主要研究方向为普适计算技术、嵌入式技术、多媒体技术、动力学系统实时数值仿真算法。