面向针对性攻击的 SDVN 控制层鲁棒性方案*

毛 明[1],伊 鹏[1],张 震[1],马 云[2]
(1.解放军战略支援部队信息工程大学,河南 郑州 450001;2.68002 部队,甘肃 兰州 730000)

摘 要:将软件定义网络应用于车联网能显著提升其性能,但该方法也面临传统 SDN 要应对的安全问题。基于软件定义车联网体系架构中控制平面可能面临的针对性节点攻击问题,提出一种鲁棒的控制器放置方法。该方法结合传统的 SDN 控制平面部署问题,首先将控制平面鲁棒性问题建模为交换机与控制器的连通冗余性问题,提升交换机在极端情形下与控制器的连通性;其次设计一个鲁棒性指标,以衡量控制平面鲁棒性。仿真结果表明,该方法的鲁棒性要优于基于时延可靠性的部署方案。

关键词:软件定义车联网;控制器部署;鲁棒性;针对性攻击
中图分类号:TN919.2;TP393.0 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.211741

中文引用格式:毛明,伊鹏,张震,等. 面向针对性攻击的 SDVN 控制层鲁棒性方案[J].电子技术应用,2022,48(2):46-50,77.
英文引用格式:Mao Ming,Yi Peng,Zhang Zhen,et al. Robust control plane scheme in SDVN toward targeted attack [J]. Application of Electronic Technique,2022,48(2):46-50,77.

Robust control plane scheme in SDVN toward targeted attack

Mao Ming[1],Yi Peng[1],Zhang Zhen[1],Ma Yun[2]
(1.People's Liberation Army Strategic Support Force Information Engineering University,Zhengzhou 450001,China;
2.68002 Troops,Lanzhou 730000,China)

Abstract:Applying software-defined networking to the Internet of Vehicles can significantly improve its performance. However, this method also faces security issues that traditional SDN has to deal with. This paper proposes a robust controller placement method based on the targeted node attack problem that the control plane may face in the software-defined vehicular networking architecture. This method combines the traditional SDN control plane deployment problem. Firstly, the control plane robustness problem is modeled as the connectivity redundancy problem between the switch and the controller. Secondly, a robustness metric is designed to measure the robustness of the control plane. The simulation results demonstrate that the robustness of this method is better than the deployment scheme based on delay reliability.

Key words:software-defined vehicular networking(SDVN);controller placement;robustness;targeted attack

0 引言

随着车联网的蓬勃发展,车载自组织网络(Vehicular Ad-hoc Network,VANET)受到工业界和学术界的极大关注。VANET 中异构无线技术灵活性、可编程性、共存性的特点,以及 5G 架构中的资源管理等可利用 SDN(Software-Defined Networking)的方式来实现[1]。

软件定义车联网(Software-Defined Vehicular Networking,SDVN)结构组成与 SDN 相似。其中控制平面由管理和控制整个网络的 SDN 控制器组成,数据平面由各种交换设备组成,在节点间实现数据转发。数据平面又分为上层数据平面和下层数据平面。上层数据平面包括支持 OpenFlow 协议的交换机和路由器,以及无线接入设施,如路边单元、基站等;下层数据平面由车辆终端用户配备的车载单元组成。与 SDN 类似,尽管分布式控制平面[2]已成为 SDVN 架构的主流设计,将控制功能集中于控制层仍然存在遭受恶意攻击的风险。

以软件定义方式解决车联网安全问题有效且富有挑战性,其不仅要解决传统 VANET 的安全问题[3-4],同时也要解决上层数据平面以上的安全问题。

目前的研究主要针对 SDN 控制平面的可靠性展开。将控制器部署问题转换为设施放置问题,被证明是一个 NP 难问题[5]。研究集中在如何在网络中选择最佳的位置来放置 K 个控制器,以实现优化目标功能最大化,例如控制器间的延迟、交换机-控制器的延迟、链路负载、

* 基金项目:国家自然科学基金项目(61802429,61872382,61521003);国家重点研发计划项目(2018YFB0804002,2019YFB1802505,2019YFB1802501,2019YFB1802502,2020YFB1804803)

控制器负载和弹性等[6-7]。也有研究从最小化控制器数量和平均延迟的组合方面来着手[8]。

本文首先将 SDVN 的控制平面抗恶意节点攻击问题归结为整形线性规划(Integer Linear Program, ILP)问题，即针对控制层与 SDVN 上层数据平面的交互与传统 SDN 数据平面的一致性，将该问题建模为 SDN 控制层的鲁棒性部署问题，并在综合考虑时延、路径连通度的基础上设计控制器放置方案。其次，提出一种控制层鲁棒性度量标准，并运用该度量标准衡量控制器放置方案对恶意节点攻击的有效性。

1 控制器放置方案建模

本研究的目标在于识别物理网络的关键部分，如何在控制层遭受节点攻击状态下，找到满足约束条件的最佳控制器位置，使得连接到控制器节点的交换机数量最大化，以提高控制平面应对针对性攻击的鲁棒性。

1.1 输入

d_{ij} 表示节点间的时延距离，l_{cc} 表示控制器与控制器间可接受的最大延迟，l_{sc} 表示交换机与控制器间可接受的最大延迟，$C=\{C_1, C_2, \cdots\}$ 表示放置控制器的节点集合，c 表示控制器数，R 表示节点集合，E 表示路径集合。$z_{ij}^{s} \in \mathbf{N}_0^+$ 为非负整数变量，表示从交换机 s 出发，经过 (i,j) 到达所有控制器的路径数目；$V(i)$ 为节点 i 的邻接节点集合。

1.2 输出

$x_{i,j} \in \{0,1\}$ 表示如果交换机 j 指向控制器 i，则为 1，否则为 0；$y_i \in \{0,1\}$ 表示如果节点 i 放置了控制器，则为 1，否则为 0；$t_{ii'} \in \{0,1\}$ 表示如果 $y_i=y_{i'}=1$，则为 1，否则为 0；α_{ij} 表示节点 i 与 j 之间的不相交路径平均数。

1.3 约束条件及放置目标

该整型线性规划的约束条件分为常规性约束条件和鲁棒性约束条件。常规性约束条件确保放置节点满足基本放置条件，鲁棒性约束确保在 $c-1$ 个控制器失联的情况下，交换机仍然有路径到达唯一幸存控制器。

常规性约束条件：

$$\sum_{i \in C,\, d_{ij} \leqslant l_{cc}} y_i \geqslant 1 \qquad \forall j \in R \tag{1}$$

$$\sum_{i \in C} x_{ij}=1 \qquad \forall j \in R \tag{2}$$

$$x_{ij} \leqslant y_j \qquad \forall i \in C,\ \forall j \in R \tag{3}$$

$$t_{ii'} d_{ii'} \leqslant l_{cc} \qquad \forall i,i' \in C \tag{4}$$

$$t_{ii'} \geqslant y_i+y_{i'}-1 \qquad \forall i,i' \in C \tag{5}$$

$$t_{ii'} \leqslant y_i \qquad \forall i,i' \in C \tag{6}$$

$$t_{ii'} \leqslant y_{i'} \qquad \forall i,i' \in C \tag{7}$$

$$x_{ij}, y_i, t_{ii'} \in \{0,1\} \tag{8}$$

式(1)确保每个交换机在可接受时延范围内都能被控制器覆盖；式(2)、式(3)确保每个交换机都只有一个控制器管理；式(4)为控制器间时延约束；式(5)~式(7)为控制器放置约束条件；式(8)定义二进制变量。

鲁棒性约束条件：

$$\sum_{j \in V(i)} (z_{ij}^{s}-z_{ji}^{s}) \leqslant y_i \qquad s \in R,\ i \in R\backslash\{s\} \tag{9}$$

$$\sum_{j \in V(i)} (z_{ij}^{s}-z_{ji}^{s}) \geqslant 0 \qquad s \in R,\ i \in R\backslash\{s\} \tag{10}$$

$$\sum_{j \in V(i)} z_{ij}^{s} \leqslant c(1-y_i) \qquad s \in R,\ i \in R \tag{11}$$

$$\sum_{j \in V(i)} z_{ji}^{s} \geqslant y_i-y_s \qquad s \in R,\ i \in R\backslash\{s\} \tag{12}$$

$$z_{is}^{s}=0 \qquad s \in R,\ i \in V(s) \tag{13}$$

$$z_{ij}^{s} \in \mathbf{N}_0^+ \qquad s \in R,\ (i,j) \in E \tag{14}$$

在 $y_i=1$ 的情况下，式(11)确保所有来自交换机 s 的路径都不穿越控制器节点；式(9)~式(11)确保最多只有一条路径到达节点 i；式(12)确保到达节点 i 的路径至少为一条；式(13)确保没有路径穿越节点 s 自身；式(14)定义节点变量域值。

放置目标函数如下：

$$\text{Maximize} \quad \sum_{j \in V(i)} \sum_{i \in C} \alpha_{ij} y_i$$

$$\text{Subject to} \quad \text{式}(1)\sim(14) \tag{15}$$

其中，α_{ij} 是控制器 i 与其相邻交换机节点 i 之间的不相交路径平均数目，本研究的目标是确保任何状态下交换机与控制器的映射数量，在控制器数目确定的情况下，应使放置目标函数最大化。

2 鲁棒的控制器部署

鲁棒的控制器部署不仅包含寻找最优控制器位置，还应根据网络流的高度动态变化实现控制器的负载均衡。因此，提出控制器域内交换机动态调整策略和鲁棒的控制器放置算法来实现鲁棒的控制器部署。

2.1 控制器域内交换机动态调整

控制器中包含流量监控模块实现流请求信息统计。由于网络中流的高度动态变化性，交换机与控制器之间的映射关系也应根据流动态变化，以确保控制器不过载。本文提出一种二次规划来选取迁移交换机和目标控制器。交换机选取应满足以下约束：

(1)选取的目标控制器容量能够容纳迁移交换机负载；

(2)应使最小数量的交换机迁移到目标控制器；

(3)迁移掉的交换机能够最大程度减少过载控制器负载。

输入：用 O 表示过载控制器集合；$\mathrm{CAP}_{\max}$ 表示控制器最大可用容量；δ_{upper} 表示控制器的负载上限比例；δ_{lower} 表示为避免过载，需考虑的控制器容量百分比；REQ_{ij} 表示控制器 i 收到的交换机 j 的流请求数；输出：CON 表示目标控制器矩阵 $(1\times(C-1))$，若 $\mathrm{con}_i=1$，则 i 为目标控制器；SW 为交换机候选矩阵 $(1\times(R-C))$，若 $\mathrm{sw}_j=1$，则该交换机

将被迁移。

首先定义约束条件如下：

$$\sum_i \mathrm{con}_i=1 \qquad \forall \in C-1 \tag{16}$$

$$\sum_j \mathrm{sw}_j=1 \qquad \forall j \in R, \mathrm{REQ}_{oj}\neq 0 \tag{17}$$

$$\sum_i \sum_{j,j\neq i} \mathrm{REQ}_{ij}\cdot \mathrm{con}_i+\sum_j \mathrm{REQ}_{oj}\cdot \mathrm{sw}_j \leqslant \delta_{\mathrm{upper}}\cdot \mathrm{CAP}_{\max} \tag{18}$$

$$d_{ij}\leqslant l_{\mathrm{sc}} \qquad \forall i \in C-1, \forall j \in R-C \tag{19}$$

$$\mathrm{con}_i \in \{0,1\} \tag{20}$$

$$\mathrm{sw}_j \in \{0,1\} \tag{21}$$

则本文所求二次规划可表示如下：

$$\text{Maximize} \sum_i \sum_j \mathrm{REQ}_{oj}\cdot \mathrm{sw}_j\cdot \mathrm{con}_i$$

$$\text{Subject to} \quad \text{式}(16)\sim(21) \tag{22}$$

目标函数(22)以寻求最大负载的交换机为目标，同时考虑时延约束(19)，因此能够使用最小数量的交换机完成迁移；式(17)和式(21)确保必有一个交换机在过载控制器域被迁移；式(18)确保目标控制器增加迁移交换机负载后的总负载满足最大可容忍负载。

本文提出算法 1，以最小数量交换机的迁移校正控制器的负载，实现网络拓扑的稳定性。二次规划的求解使用 CPLEX[9]来实现。

算法 1 交换机重定向算法

输入：现有交换机–控制器映射关系，$\mathrm{CAP}_{\max}$，δ_{upper}，δ_{lower}，REQ_{ij}；

输出：新的映射关系。

```
if δ ⩾ δ_upper · CAP_max
    使用 CPLEX 在约束(16)~(21)下求解式(22)
    迁移得到的交换机到目标控制器
    计算迁移后的控制器负载
    if 控制器剩余负载 ⩾ δ_lower · CAP_max
       继续求解该二次规划
    else
       导出待迁移的交换机、数量及目标控制器
    end if
end if
```

2.2 控制器放置算法

该算法包含 3 个步骤：(1)由于控制器数是给定的，利用 ILP 求解器 CPLEX 求出符合条件的控制器集合 C；(2)由于本文的重点在于研究控制层鲁棒性，为实现控制器域的快速划分，划分工作使用完全搜索算法[10]来实现；(3)若域内控制器负载超出设定域值，则通过交换机重定向来实现负载调整。下面给出鲁棒的控制器放置(Robust Controller Placement，RCP)实现算法。

算法 2 鲁棒的控制器放置算法(RCP)

输入：控制器拓扑 $G(V,E)$，控制器数 c，交换机节点集合 S，节点间延迟 d_{ij}，控制器负载 δ；

输出：控制器位置集合 C，交换机–控制器映射关系 s_m^i。

```
C←根据控制器数量 c，在约束(1)~(14)下，使用 CPLEX 求解控制器集合 C；
s_m^i ←Ø
for C_i ∈ C
    if S ≠ Ø then
      ∀s_j ∈ S
        根据约束 d_ij ⩽ l_sc，选取 m=arg min d_ij
        s_m^i = s_m^i ∪ m
        S←S−s_m^i
      end if
    if δ_i ⩾ δ_upper · CAP_max
        利用算法 1 对控制器域内交换机重定向
    end if
        更新 s_m^i
end for
```

3 性能评估

由于本文的目标是在攻击状态时，尽可能确保每个交换机都有到达幸存控制器的路径，因此使用网络中所有节点对的平均对端可达性(Average Terminal Reachability，ATR)作为衡量控制层鲁棒性的指标。该指标物理含义为网络中相互连通的节点对所占比例。设 M 为网络被分割的区域数，m_i 为被分割区域内的节点数，N 为网络节点总数，则 ATR 公式表达如下：

$$\mathrm{ATR}=\frac{\sum_{i=1}^{M} m_i(m_i-1)}{N(N-1)} \tag{23}$$

当网络节点完全连通时，该取值为 1；否则，对各分割区域的节点对数求和，并除以节点对总数。当节点设备被移除数目增加时，该取值将逐渐趋近于 0。

3.1 鲁棒性分析

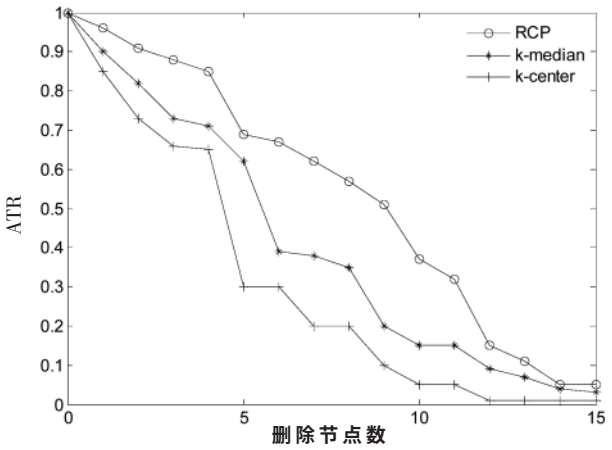
文献[11]指出，通过网络拓扑结构可以确定哪些针对性攻击将产生最大的破坏。因此，本文采取移除中心性度量值最大的节点的方法来模拟攻击。本文使用 3 种攻击度量[12]，分别称为度中心性(Degree Centrality Attack，DCA)、紧密中心性(Closeness Centrality Attack，CCA)和介数中心性攻击(Betweenness Centrality Attack，BCA)。其中，度中心性攻击的目标是具有最多邻居节点数的节点；紧密中心性攻击的目标是基于最短路径的最接近其他节点的节点；介数中心性攻击的目标是出现在其他节点之间最短路径数最多的节点。

Heller 等人指出单控制器已能够应对中等规模网络的正常运转[5]，为确保 CPLEX 求解时间可接受，参考文献[13]的结论，将控制器数 c 设为 5 个。为方便对比，使用 Heller 的 k–median 与 k–center 方案与鲁棒性放置方

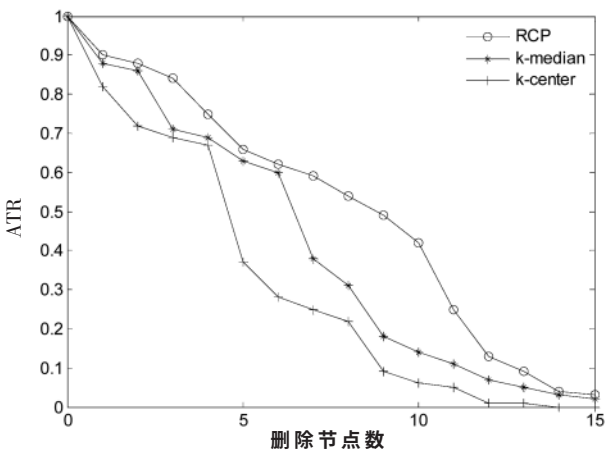
案作对比，其中控制器容量上限 δ_{upper} 设为 0.9，δ_{lower} 设为 0.7。使用两种网络拓扑来验证提出的鲁棒性方案，其中拓扑 janos-us-ca 拥有 39 个节点、122 条链路，平均节点度为 6.26；拓扑 sprint 拥有 97 个节点、379 条链路，平均节点度为 5.42。针对 3 种不同的攻击方式，随移除节点数目变化，计算网络 ATR 值。

首先对比在 janos-us-ca 中 ATR 值的变化，如图 1 所示。移除节点为 10 时，当实施 DCA 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 22%和 31%；当实施 CCA 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 28%和 36%；当实施 BCA 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 28%和 34%。当移除节点达到 15 及以上时，ATR 值趋近于 0。

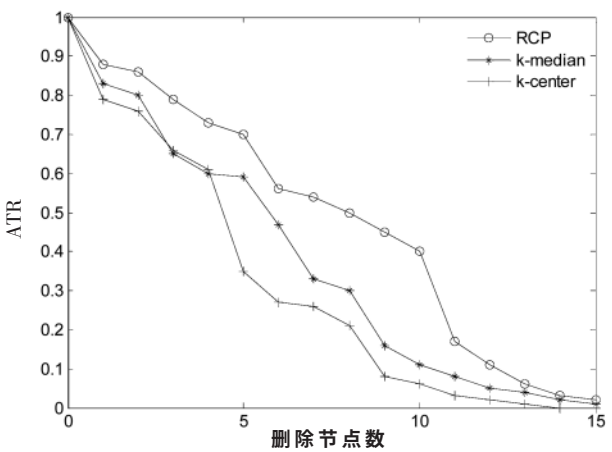
其次分析在 sprint 中 ATR 值的变化，如图 2 所示。



(a)janos-us-ca 中的 DCA 时的 ATR 值

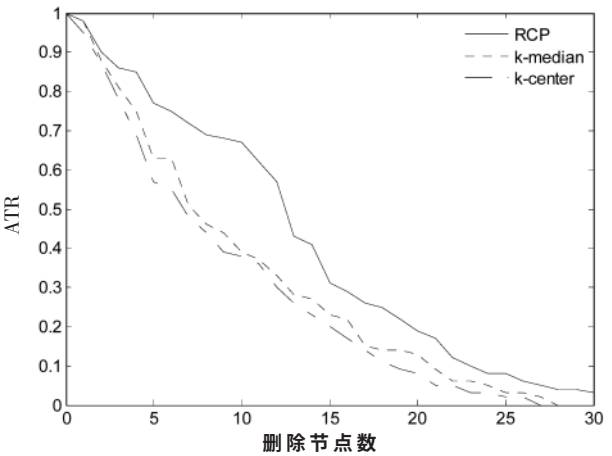


(b)janos-us-ca 中 CCA 时的 ATR 值

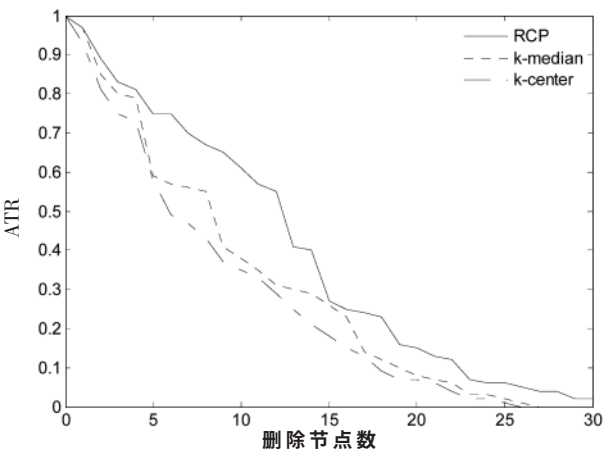


(c)janos-us-ca 中 BCA 时的 ATR 值

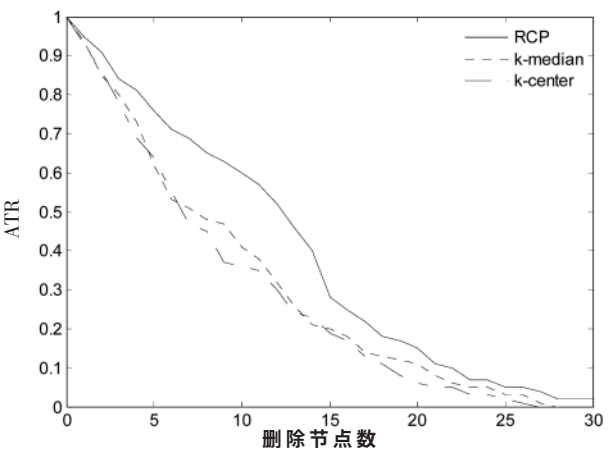
图 1 janos-us-ca 中的 ATR 值变化



(a)sprint 中 DCA 时的 ATR 值



(b)sprint 中 CCA 时的 ATR 值



(c)sprint 中 BCA 时的 ATR 值

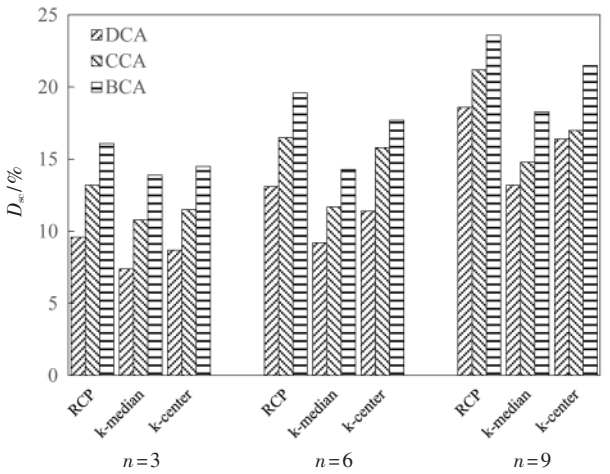
图 2 sprint 中的 ATR 值变化

实施 DCA 时，当移除节点为 20 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 6%和 11%；当实施 CCA 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 7%和 8%；当实施 BCA 时，RCP 的 ATR 值分别比 k-median 和 k-center 高 4%和 9%。当移除节点数达到 30 及以上时，ATR 值趋近于 0。

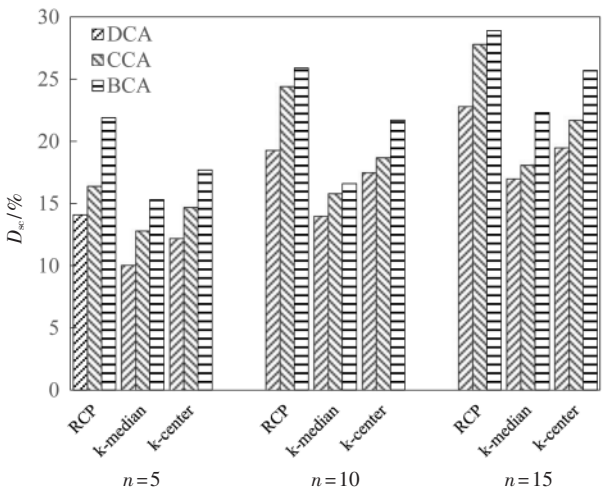
如果用数据曲线的覆盖面积大小衡量控制层鲁棒性高低，可以得到相同的结论，即 RCP 的鲁棒性要优于 k-median 和 k-center。

3.2 时延分析

本文定义攻击状态下的时延 D_{sc} 为：活跃交换机到控制器的平均最短路径长度与拓扑图直径的比值。记移除节点数为 n，分别计算 janos-us-ca 中 n 取值为 3、6、9 时，sprint 中 n 取值为 5、10、15 时，两种网络拓扑的时延。实验结果如图 3 所示。



(a) janos-us-ca 中时延对比



(b) sprint 中时延对比

图 3 两种网络拓扑时延

通过对比能够发现，各放置方法在相同攻击条件下的时延特性是一致的。其中 K-median 方法的时延最低，这是由于该方法以最小化平均最短路径为目标。相比其他两种方法，鲁棒性放置方法时延较高。这是由于尽管鲁棒性放置方法优化目标针对提高控制平面鲁棒性，但其也考虑了时延约束，由此带来的延迟损失在可容忍范围内。

4 结论

本文针对软件定义车联网中控制平面可能遭受的恶意节点攻击问题，提出了一种鲁棒的控制器部署方案并建模，通过约束规则确保控制平面的鲁棒性，同时使用 CPLEX 工具求解，简化了算法复杂度。实验结果表明，与考虑可靠性指标的部署方法相比，该方案在应对 3 种攻击时提升控制平面鲁棒性方面优于 k-median 和 k-center。

参考文献

[1] CARDONA N, CORONADO E, LATRE S, et al. Software-defined vehicular networking: opportunities and challenges[J]. IEEE Access, 2020, 8: 219971-219995.

[2] KAZMI A, KHAN M A, AKRAM M U. DeVANET: decentralized software-defined VANET architecture[C]//2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 2016: 42-47.

[3] YANG L. Security and privacy in the Internet of Vehicles[C]// International Conference on Identification. IEEE, 2017.

[4] FRAIJI Y, AZZOUZ L B, TROJET W, et al. Cyber security issues of Internet of electric vehicles[C]//2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 2018: 1-6.

[5] HELLER B, SHERWOOD R, MCKEOWN N. The controller placement problem[C]//Workshop on Hot Topics in Software Defined Networks. ACM, 2012.

[6] LANGE S, GEBERT S, ZINNER T, et al. Heuristic approaches to the controller placement problem in large scale SDN networks[J]. IEEE Transactions on Network & Service Management, 2017, 12(1): 4-17.

[7] NENCIONI G, HELVIK B E, HEEGAARD P E. Including failure correlation in availability modeling of a software-defined backbone network[J]. IEEE Transactions on Network & Service Management, 2017, PP(4): 1.

[8] PERROT N, REYNAUD T. Optimal placement of controllers in a resilient SDN architecture[C]//International Conference on the Design of Reliable Communication Networks. IEEE, 2016: 145-151.

[9] IBM. IBM CPLEX optimizer[EB/OL]. [2021-05-11]. https://www.ibm.com/cn-zh/analytics/cplex-optimizer.

[10] HOLLINGHURST J, GANESH A, BAUGÉ T. Controller placement methods analysis[C]//2016 6th International Conference on Information Communication and Management (ICICM), Hatfield, UK, 2016: 239-244.

[11] RUEDA D F, CALLE E, MARZO J L. Robustness compa-

(下转第 77 页)

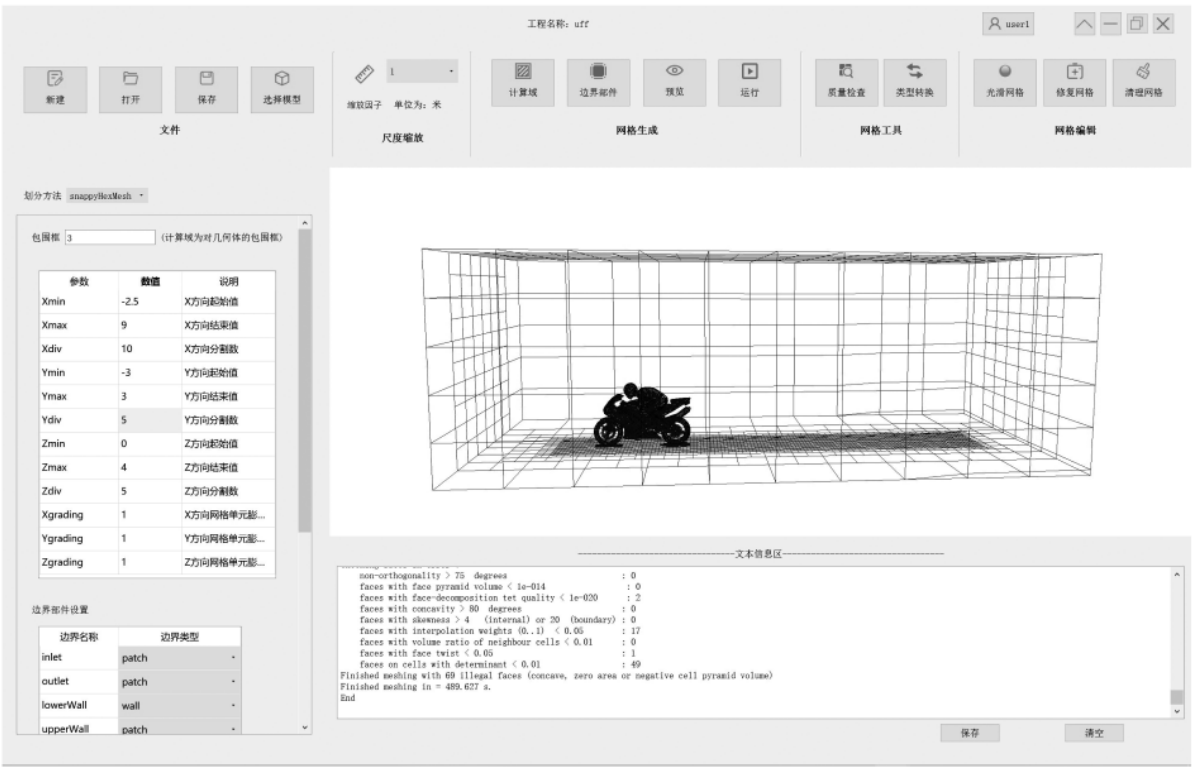


图 4　客户端软件主界面(motorBike 算例)

综述[J].计算机工程与应用,2021,57(2):1-11.

[8] 崔晨.基于 OpenFOAM 的网格划分评估与优化[D].长沙:国防科技大学,2017.

[9] Guan Shiqi,Hu Wenshan,Zhou Hong.Real-time data transmission method based on websocket protocol for networked control system laboratory[C]//NNSF,2019:5339-5344.

[10] 蔡增玉,王文倩,赵振宇,等.基于 H.265 的云机器人图像采集系统设计与实现[J].现代电子技术,2021,44(5):66-69.

[11] 陈永当,马柯,刘斌,等.一种功能可配置的业务中间件软件产品及其应用[J].计算机应用与软件,2012,29(6):145-147,175.

[12] 陈凯翔.基于眼动交互的用户界面设计与研究[D].北京:北京邮电大学,2018.

[13] 鲁阳,王腾.持续集成模式下软件配置管理方法与实践[J].西北工业大学学报,2019,37(S1):68-73.

[14] 王晓辉,聂小华,常亮.基于 Qt 的专用有限元软件 GUI 模块的设计与开发[J].计算机应用与软件,2010,37(1):21-26,65.

[15] 徐建明,俞俊铭,董建伟,等.基于云平台的机器人监控系统设计[J].高技术通讯,2020,30(9):938-948.

(收稿日期:2021-03-15)

作者简介:

张志达(1994-),男,硕士研究生,主要研究方向:智能信息处理。

淮晓永(1973-),男,博士,高级工程师,主要研究方向:智能软件工程、云计算。

高若辰(1996-),女,硕士研究生,主要研究方向:智能信息处理。

扫码下载电子文档

(上接第 50 页)

rison of 15 real telecommunication networks: structural and centrality measurements[J].Journal of Network and Systems Management,2017,25(2):269-289.

[12] SWAMI I,TIMOTHY K,BALA S,et al.Attack robustness and centrality of complex networks[J].Plos One,2013,8(4):e59613.

[13] ROS F J,RUIZ P M.On reliable controller placements in software-defined networks[J].Computer Communications,2016,77:41-51.

(收稿日期:2021-05-11)

作者简介:

毛明(1987-),男,博士研究生,主要研究方向:网络安全、车联网安全。

伊鹏(1977-),男,研究员,主要研究方向:网络安全、车联网安全。

张震(1985-),男,副教授,主要研究方向:网络安全。

扫码下载电子文档

版权声明