CF-MARLOS: یادگیری تقویتی چندعامله فدرالِ همکارانه با تجمیع آموختنی برای تشخیص نفوذ مجموعه‌باز در ترافیک B-NAT

محمد حسن امینی
دانشجوی کارشناسی ارشد، دانشگاه علم و صنعت ایران
m_amini79@cmps2.iust.ac.ir

چکیده

این مقاله چارچوب CF-MARLOS را برای تشخیص نفوذ در ترافیک B-NAT تحت یادگیری فدرال افقی و داده‌های غیرهمسان ارائه می‌کند. سامانه پیشنهادی سه جزء را به‌صورت هم‌زمان ترکیب می‌کند: عامل محلی CVAE-DQN برای طبقه‌بندی کلاس‌های شناخته‌شده، لایه تجمیع فدرال برای حفظ حریم خصوصی و مقیاس‌پذیری، و واسنجی EVT برای رد نمونه‌های ناشناخته. در این معماری، فقط پارامترهای یادگیریِ مشترک میان کلاینت‌ها فدرال می‌شوند؛ حافظه بازپخش، وضعیت بهینه‌ساز، داده خام و مصنوعات EVT محلی یا پساآموزشی باقی می‌مانند. پس از آموزش فدرال، مدل جهانی با خطاهای بازسازیِ نمونه‌های اعتبارسنجیِ درست‌طبقه‌بندی‌شده واسنجی می‌شود تا بتواند حملات دیده‌نشده را با آستانه‌ای کنترل‌شده رد کند. این طراحی برای بهبود هم‌زمانِ دقت کلاس‌های شناخته‌شده، پایداری تحت ناهمگنی کلاینتی، و تشخیص مجموعه باز مناسب است.

کلیدواژه‌ها: یادگیری فدرال، تشخیص نفوذ، تشخیص مجموعه باز، EVT، Double DQN، ترافیک B-NAT

۱ مقدمه

ترافیک B-NAT و سامانه‌های توزیع‌شده مشابه، به‌طور طبیعی در چندین گره، سازمان یا نقطه پایش جداگانه ذخیره می‌شوند. در چنین محیط‌هایی، متمرکز کردن داده خام همواره ممکن یا مطلوب نیست. یادگیری فدرال یک راه‌حل طبیعی فراهم می‌کند، اما قواعد تجمیع استاندارد مانند FedAvg در حضور توزیع‌های غیرهمسان می‌توانند ناپایدار شوند. دشواری مسئله در تشخیص نفوذ بیشتر می‌شود، زیرا مدل نه‌تنها باید حملات شناخته‌شده را طبقه‌بندی کند، بلکه باید حملات دیده‌نشده را نیز به‌درستی رد کند.

پیاده‌سازی این پروژه یک خط لوله ترکیبی را دنبال می‌کند که در آن یادگیری بازنمایی نهفته، Double DQN، مولد بازسازی، و EVT در یک معماری فدرال همکارانه ادغام شده‌اند. در این مقاله، CF-MARLOS به‌عنوان یک روش یکپارچه برای طبقه‌بندی مجموعه بسته، رد ناشناخته و آموزش فدرال تحت ناهمگنی کلاینتی ارائه می‌شود.

۲ پیشینه و صورت مسئله

در این چارچوب، هر کلاینت مجموعه داده محلی D_i را در اختیار دارد و داده خام را با سرور به اشتراک نمی‌گذارد. هدف فدرال، کمینه‌سازی مجموع وزن‌دار زیان‌های محلی است:

$$\min_{\Theta} \sum_{i=1}^{N} \frac{n_i}{\sum_j n_j} F_i(\Theta),$$

که در آن n_i تعداد نمونه‌های محلی کلاینت i است. در حالت FedProx، هدف محلی با جمله پروگزیمال به‌صورت زیر اصلاح می‌شود:

$$F_i^{\text{prox}}(\Theta) = F_i(\Theta) + \frac{\mu}{2}\|\Theta - \Theta^{k-1}\|_2^2.$$

برای تشخیص مجموعه باز، به‌جای اتکا به اعتماد نرمِ مجموعه بسته، از خطای بازسازی و مدل‌سازی دم EVT استفاده می‌شود. این کار به مدل اجازه می‌دهد تا نمونه‌هایی را که به توزیع کلاس‌های شناخته‌شده تعلق ندارند، با آستانه‌ای واسنجی‌شده رد کند.

۳ روش‌شناسی پیشنهادی

۱.۳ نمای کلی سامانه

شکل ۱ نمای کلی CF-MARLOS را نشان می‌دهد. ترافیک خام B-NAT از CSV به مصنوعات تانسوری تبدیل می‌شود، کلاس‌های شناخته‌شده به فضای برچسب ثابت نگاشت می‌شوند، و داده آموزش به قطعات کلاینتی غیرهمسان تقسیم می‌شود. هر کلاینت فقط قطعه خود را مشاهده می‌کند و عامل CVAE-DQN محلی را آموزش می‌دهد. سرور در هر دور فقط پارامترهای مدل یا خلاصه‌های ممیزی را دریافت می‌کند، آن‌ها را تجمیع می‌کند، و در پایان آموزش، مدل جهانی را با EVT واسنجی می‌کند. برای سازگاری میان نسخه انگلیسی و فارسی مقاله، همین شکل انگلیسی در هر دو نسخه استفاده شده است.

۲.۳ عامل محلی CVAE-DQN

فرض کنید $s \in \mathbb{R}^d$ بردار ویژگی ترافیک و $a \in \{1, \ldots, C\}$ یکی از کلاس‌های شناخته‌شده باشد. هر کلاینت مسئله را به‌صورت یک فرمول‌بندی تقویتیِ مبتنی بر مخزن داده مدل می‌کند؛ در این فرمول‌بندی، کنش همانِ کلاس پیش‌بینی‌شده است و پاداش با درستیِ پیش‌بینی تعیین می‌شود.

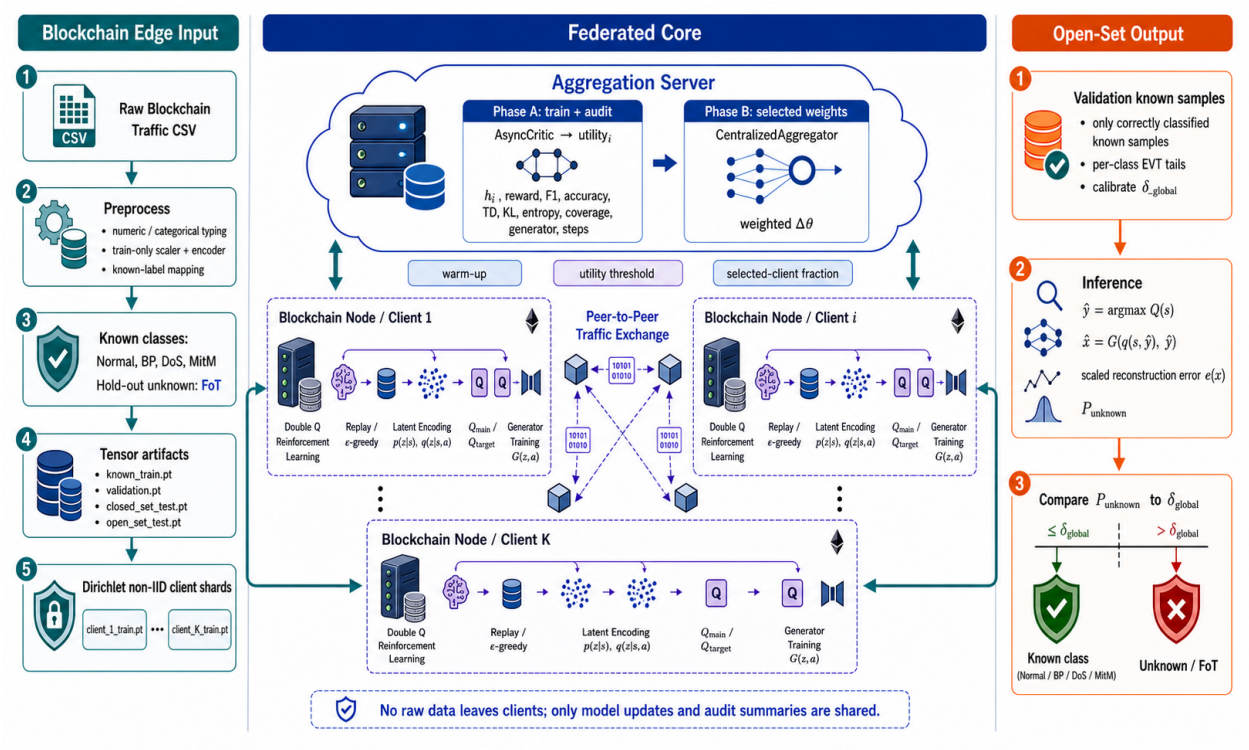
عامل محلی از چهار مؤلفه اصلی تشکیل شده است:

- شبکه پیشین $p_\theta(z \mid s)$ برای نگاشت حالت به توزیع نهفته؛
- شبکه بازشناسی $q_\phi(z \mid s, a)$ برای استنتاج نهفته وابسته به کلاس؛
- شبکه Q اصلی $Q_\psi(z, s)$ برای انتخاب کلاس شناخته‌شده؛
- شبکه Q هدف $Q_{\psi^-}(z, s)$ برای پایدارسازی Double DQN؛
- مولد $G_\omega(z, a)$ برای بازسازی ویژگی‌ها.

شبکه پیشین با شبکه بازشناسی هم‌تراز می‌شود:

$$L_{\text{prior}} = \mathrm{KL}(q_\phi(z \mid s, a^*) \,\|\, p_\theta(z \mid s)).$$

برای به‌روزرسانی TD، از هدف Double DQN استفاده می‌شود:



شکل ۱: نمای کلی CF-MARLOS: پیش‌پردازش، قطعه‌های غیرهمسان کلاینتی، آموزش محلی CVAE-DQN، تجمیع فدرال، و استنتاج مجموعه‌باز مبتنی بر EVT.

$$a' = \arg\max_{a} Q_{\psi}(z', s', a),$$
$$y = r + \gamma(1-d)\, Q_{\psi^-}(z', s', a').$$

$$L_{\text{TD}} = \text{Huber}(Q_{\psi}(z, s, a) - y)\,.$$

بازپخش تجربه و سیاست ϵ-حریصانه برای یادگیری محلی استفاده می‌شوند. شبکه هدف فقط به‌صورت محلی همگام می‌شود و به‌عنوان یک مؤلفه فدرال مستقل ارسال نمی‌شود. اگر FedProx فعال باشد، جمله پروگزیمال زیر نیز به هدف محلی افزوده می‌شود:

$$L_{\text{prox}} = \frac{\mu}{2}\|\Theta_i - \Theta^{k-1}\|_2^2.$$

۳.۳ بازسازی مبتنی بر مولد

مولد پس از پیش‌بینی کلاس، نمونه را به‌صورت شرطی بازسازی می‌کند:

$$\hat{x} = G_{\omega}(z, \hat{a}), \qquad e(x) = \frac{1}{d}\|x - \hat{x}\|_2^2 \cdot \kappa.$$

مولد فقط روی نمونه‌های شناخته‌شده و درست‌طبقه‌بندی‌شده آموزش داده می‌شود. این انتخاب باعث می‌شود فضای بازسازی به منیفلد کلاس‌های شناخته‌شده نزدیک بماند و خطای بازسازی برای نمونه‌های ناشناخته، سیگنال معنادارتری داشته باشد.

جدول ۱: مؤلفه‌های فدرال‌شده و فدرال‌نشده در CF-MARLOS

مؤلفه فدرال‌شده	نقش
شبکه پیشین $p_{\theta}(z\|s)$	بازنمایی نهفته مشترک
شبکه بازشناسی $q_{\phi}(z\|s,a)$	استنتاج نهفته و بازسازی
شبکه Q اصلی $Q_{\psi}(z,s)$	سیاست جهانی کلاس‌های شناخته‌شده
مولد $G_{\omega}(z,a)$	رفتار بازسازی مشترک
مؤلفه فدرال‌نشده	**نقش**
شبکه Q هدف Q_{ψ^-}	کپی محلی برای پایدارسازی
حافظه بازپخش	تاریخچه محلی گذارها
وضعیت بهینه‌ساز	وضعیت خصوصی آموزش
مدل‌ها و آستانه‌های EVT	مصنوعات واسنجی پساآموزشی
داده خام کلاینت	روی کلاینت باقی می‌ماند

۴.۳ اشتراک‌گذاری پارامترها

در CF-MARLOS، فقط پارامترهای یادگیریِ مشترک فدرال می‌شوند:

این مرزبندی به حفظ حریم خصوصی، کاهش هزینه ارتباطی، و جلوگیری از تجمیع اشیای گذرای محلی کمک می‌کند.

۵.۳ FedAvg و FedProx به‌عنوان مبنا

FedAvg از میانگین وزن‌دار بر اساس تعداد نمونه استفاده می‌کند:

الگوریتم ۱ آموزش فدرال CVAE-DQN و واسنجی مجموعه‌باز

ورودی: مجموعه داده‌های کلاینت‌ها $\{D_i\}_{i=1}^N$، مجموعه اعتبارسنجی D_{val}، تعداد دورها K، پیکربندی محلی H، و راهبرد $S \in \{\text{FedAvg}, \text{FedProx}, \text{FMRL-LA}\}$

خروجی: مدل نهایی θ^*، مدل‌های EVT M_{evt}، و آستانه رد δ

پارامترهای اولیه $\theta^0 = \{\theta_p^0, \theta_r^0, \theta_Q^0, \theta_G^0\}$ را مقداردهی کن

برای $k = 1$ تا K **انجام بده**

سرور کلاینت‌های C_k را نمونه‌گیری کرده و θ^{k-1} را به آن‌ها پخش می‌کند

برای هر $i \in C_k$ **به‌صورت موازی انجام بده**

$\mu_i \leftarrow \mu$ اگر $S = \text{FedProx}$ باشد، و در غیر این صورت $\mu_i \leftarrow 0$

$(\theta_i^k, m_i^k) \leftarrow \text{ClientLocalUpdate}(D_i, \theta^{k-1}, H, \mu_i)$

پایان برای

اگر $S = \text{FMRL-LA}$ **آنگاه**

$\theta^k \leftarrow \text{FMRLLAUpdate}(\theta^{k-1}, \{(\theta_i^k, m_i^k)\})$

وگرنه

$\theta^k \leftarrow \frac{\sum_{i \in C_k} n_i \theta_i^k}{\sum_{i \in C_k} n_i}$

پایان اگر

پایان برای

$\theta^* \leftarrow \theta^K$

$(M_{\text{evt}}, \delta) \leftarrow \text{EVTCalibration}(D_{\text{val}}, \theta^*)$

بازگردان $\theta^*, M_{\text{evt}}, \delta$

الگوریتم ۲ به‌روزرسانی محلی CVAE-DQN با گزینه FedProx

ورودی: داده محلی D_i، پارامترهای پخش‌شده θ^{k-1}، پیکربندی محلی H، و ضریب پروگزیمال μ_i

خروجی: پارامترهای به‌روزشده θ_i^k و شاخص‌های ممیزی m_i^k

θ^{k-1} را در p_θ، q_ϕ، Q_ψ و G_ω بارگذاری کن

شبکه هدف را با $Q_\psi \leftarrow Q_\psi^-$ مقداردهی کرده و θ^{k-1} را مرجع FedProx قرار بده

حافظه بازپخش B_i و سیاست ϵ-حریصانه π_i را مقداردهی کن

برای هر اپیزود محلی **انجام بده**

با محیط محلی تعامل کن و گذارهای $(s_t, a_t, r_t, s_{t+1}, d_t, a_t^*)$ را در B_i ذخیره کن

اگر $|B_i|$ کافی باشد **آنگاه**

یک مینی‌بچ از B_i نمونه‌گیری کن

p_θ را با L_{prior} و در صورت فعال بودن با جریمه FedProx به‌روزرسانی کن

q_ϕ و Q_ψ را با L_{TD} و در صورت فعال بودن با جریمه FedProx به‌روزرسانی کن

Q_ψ^- را به‌صورت نرم یا دوره‌ای از Q_ψ همگام کن

پایان اگر

پایان برای

مجموعه نمونه‌های شناخته‌شده و درست‌طبقه‌بندی‌شده را بساز

اگر آموزش مولد فعال باشد **آنگاه**

G_ω را فقط روی نمونه‌های شناخته‌شده و درست‌طبقه‌بندی‌شده آموزش بده

پایان اگر

بازگردان $\theta_i^k = \{\theta_p, \theta_r, \theta_Q, \theta_G\}$ و m_i^k

$$\Theta^k = \sum_{i \in C_k} \frac{n_i}{\sum_{j \in C_k} n_j} \Theta_i^k.$$

FedProx همان منطق سمت سرور را حفظ می‌کند، اما با جمله پروگزیمال، انحراف به‌روزرسانی‌های محلی را محدود می‌سازد. FedAvg و FedProx در این مقاله مبنا هستند و به‌عنوان مشارکت اصلی روش پیشنهادی تلقی نمی‌شوند.

۶.۳ تجمیع همکارانه FMRL-LA

FMRL-LA مؤلفه نوآورانه اصلی این کار است. این روش به‌جای فرض مساوی بودن تمام کلاینت‌ها، سودمندی هر کلاینت را پیش از تجمیع برآورد می‌کند. در فاز A، کلاینت‌ها محلی آموزش می‌بینند و فراداده ممیزی شامل پاداش، F1، دقت، پایداری TD، نوآوری مبتنی بر KL، آنتروپی، پوشش برچسب، کیفیت مولد و تعداد گام‌ها را ارسال می‌کنند. سرور این اطلاعات را با یک منتقد ناهمگام ارزیابی می‌کند و امتیاز سودمندی u_i را به دست می‌آورد.

در فاز B، کلاینت‌های منتخب وزن‌های ذخیره‌شده را می‌فرستند و سرور دلتاهای پارامتری را با وزن سودمندی تجمیع می‌کند:

$$\Delta_i = \Theta_i^k - \Theta^{k-1}, \qquad \Theta^k = \Theta^{k-1} + \eta \frac{\sum_{i \in A_k} u_i \Delta_i}{\sum_{i \in A_k} u_i}.$$

این طرح، به‌ویژه در داده‌های غیرهمسان، می‌تواند پایداری و کارایی ارتباطی را بهتر کند. در مقابل، هزینه آن افزایش هماهنگی است، زیرا هر دور منطقی شامل دو فاز جداگانه است.

۷.۳ واسنجی EVT و استنتاج مجموعه باز

پس از آموزش فدرال، مدل جهانی با EVT واسنجی می‌شود. فقط نمونه‌های اعتبارسنجیِ شناخته‌شده و درست‌طبقه‌بندی‌شده برای برازش دم استفاده می‌شوند. برای هر کلاس، دم بالایی خطای بازسازی با توزیع پارتوی تعمیم‌یافته مدل می‌شود و سپس احتمال ناشناختگی محاسبه می‌گردد:

$$P_{\text{unknown}}(x) = M_{\text{EVT},\hat{a}}(e(x)).$$

آستانه جهانی δ_{global} از داده اعتبارسنجی تنظیم می‌شود. در زمان استنتاج، اگر

$$P_{\text{unknown}}(x) < \delta_{\text{global}},$$

نمونه به‌عنوان کلاس شناخته‌شده پذیرفته می‌شود؛ در غیر این صورت به‌عنوان ناشناخته رد می‌شود. این مرحله مدل را از طبقه‌بند مجموعه بسته به آشکارساز نفوذ مجموعه باز تبدیل می‌کند.

۸.۳ تحلیل الگوریتم‌ها

الگوریتم ۱ جریان کامل آموزش فدرال و واسنجی نهایی را خلاصه می‌کند و نشان می‌دهد که آموزش فدرال و کالیبراسیون EVT دو مرحله متمایز ولی پیوسته هستند. الگوریتم ۲ به‌روزرسانی محلی CVAE-DQN را با یا بدون FedProx مشخص می‌کند و روشن می‌سازد که شبکه هدف فقط نقش پایدارسازی محلی دارد. الگوریتم ۳ قاعده انتخاب و تجمیع FMRL-LA را توضیح می‌دهد و مزیت آن را در مواجهه با ناهمگنی کلاینتی نشان می‌دهد. الگوریتم ۴ نیز برازش EVT و تصمیم‌گیری مجموعه‌باز را در مرحله استنتاج ارائه می‌کند.

الگوریتم ۳ انتخاب و تجمیع آگاه از سودمندی در FMRL-LA

ورودی: پارامترهای جهانی قبلی θ^{k-1}، به‌روزرسانی‌ها و شاخص‌های کلاینتی $\{(\theta_i^k, m_i^k)\}$، آستانه سودمندی λ، حداقل کلاینت منتخب $q_{\min}$، حداکثر نسبت $\rho_{\max}$، و نرخ گام η

خروجی: پارامترهای جهانی به‌روزشده θ^k

سودمندی u_i را برای هر کلاینت با استفاده از خلاصه‌های نهفته و شاخص‌ها برآورد کن

مجموعه $A_k = \{i : u_i \geq \lambda\}$ را انتخاب کن

اگر $|A_k| < q_{\min}$ **آنگاه**

کلاینت‌های با بیشترین سودمندی را اضافه کن تا $|A_k| = q_{\min}$ شود

پایان اگر

$|A_k| \leq \lceil \rho_{\max}|C_k| \rceil$ را اعمال کن

برای هر $i \in A_k$ **انجام بده**

$\Delta_i \leftarrow \theta_i^k - \theta^{k-1}$

پایان برای

$\theta^k \leftarrow \theta^{k-1} + \eta \frac{\sum_{i \in A_k} u_i \Delta_i}{\sum_{i \in A_k} u_i}$

منتقدهای سمت سرور و مخلوط‌کننده را با بازخورد سودمندی دور به‌روزرسانی کن

بازگردان θ^k

۹.۳ منطق طراحی

هر مؤلفه در CF-MARLOS یک شکست مشخص را هدف می‌گیرد: عامل CVAE-DQN رفتار طبقه‌بندی مجموعه بسته را می‌آموزد، مولد سیگنال بازسازی را فراهم می‌کند، لایه فدرال آموزش توزیع‌شده را ممکن می‌سازد، FMRL-LA ناهمگنی کلاینتی را مدیریت می‌کند، و EVT قانون ردِ واسنجی‌شده را برای حملات ناشناخته ارائه می‌دهد. این جداسازی وظایف، روش را برای آزمایش‌های حذف مؤلفه، تحلیل حساسیت، و تحلیل کارایی مناسب می‌سازد.

۴ پیکربندی تجربی

پروتکل ارزیابی مطابق قرارداد مخزن تنظیم شده است. داده اصلی، ترافیک بلاکچین B-NAT است. در تنظیم مجموعه‌باز، کلاس‌های «نرمال»، «بی‌پی»، «دی‌اواس» و «میتم» به‌عنوان کلاس‌های شناخته‌شده در نظر گرفته می‌شوند و «فوت» به‌عنوان حمله ناشناخته نگه داشته می‌شود. برای نسخه نهایی، تنظیم اصلی شامل ۱۰ کلاینت و ۱۰۰ دور منطقی فدرال است؛ تنظیمات کوچک‌تر فقط برای آزمون‌های سریع و توسعه در مخزن باقی مانده‌اند.

تمام مقایسه‌ها از همان قرارداد پیش‌پردازش، همان تقسیم آموزش/اعتبارسنجی/آزمون، همان بذرهای تصادفی، و همان قطعات کلاینتی استفاده می‌کنند. قطعات غیرهمسان با نمونه‌گیری دایریکله روی برچسب کلاس‌ها ساخته می‌شوند و $\alpha \in \{0.01, 0.5, 1.0\}$ برای کنترل ناهمگنی به‌کار می‌رود. مبناهای اصلی شامل آموزش متمرکز، آموزش محلی، FedAvg، FedProx، و FMRL-LA هستند. پیکربندی اجرا از طریق Hydra کنترل می‌شود و شامل تعداد اپیزودهای محلی در هر دور، اندازه حافظه بازپخش، اندازه بچ، تنظیمات Double DQN، آموزش مولد، و پرچم‌های واسنجی مجموعه‌باز است.

پروتکل نهایی باید به هفت آزمایش سازمان‌دهی شود: اعتبارسنجی مجموعه بسته، تشخیص مجموعه‌باز، مقایسه فدرال غیرهمسان، ارزیابی هم‌زمان مجموعه‌باز و غیرهمسان، حذف مؤلفه و حساسیت، کارایی و مقیاس‌پذیری، و آزمون استرس مجموعه‌باز برحسب برچسب. این ساختار، روایت مقاله را از سطح پیاده‌سازی به سطح سؤال پژوهشی منتقل می‌کند.

الگوریتم ۴ واسنجی EVT و استنتاج مجموعه باز

ورودی: مجموعه اعتبارسنجی D_{val}، مدل آموزش‌دیده θ^*، کسر دُم α_{evt}، و نرخ مثبت کاذب هدف β

خروجی: مدل‌های EVT M_{evt}، آستانه جهانی δ، و پیش‌بینی نهایی $\hat{y}$

خطاهای بازسازی نمونه‌های شناخته‌شده و درست‌طبقه‌بندی‌شده را جمع‌آوری کن

برای هر کلاس‌های شناخته‌شده c **انجام بده**

یک مدل دُم EVT را برای دُم بالایی خطاهای کلاس c برازش کن

پایان برای

احتمالات ناشناختگی روی داده اعتبارسنجی را تخمین بزن و δ را از کمیتِ $(1-\beta)$ تعیین کن

برای هر نمونه استنتاجی x **انجام بده**

کلاس پیش‌بینی‌شده $\hat{c} = \arg\max_c Q_\psi(p_\theta(x), x, c)$ را محاسبه کن

خطای بازسازی e_x را با q_ϕ و G_ω محاسبه کن

$p_u = M_{\text{evt}}[\hat{c}](e_x)$ را محاسبه کن

اگر $p_u \geq \delta$ **آنگاه**

$\hat{y} \leftarrow$ ناشناخته

وگرنه

$\hat{y} \leftarrow \hat{c}$

پایان اگر

پایان برای

بازگردان $M_{\text{evt}}, \delta, \hat{y}$

۵ معیارهای ارزیابی

در ارزیابی مجموعه بسته، باید دقت، macro precision، macro recall، macro F1، weighted F1، دقت متوازن، و ماتریس‌های سردرگمی گزارش شوند. این معیارها نشان می‌دهند که مدل قبل از اعمال ردِ مجموعه‌باز، تا چه حد کلاس‌های شناخته‌شده را درست تفکیک می‌کند.

در ارزیابی مجموعه‌باز، باید AUROC، AUPRC، FPR@95%TPR، TPR@5%FPR، unknown F1، نرخ رد ناشناخته، و دقت کلاس‌های شناخته‌شده پس از رد گزارش شوند. این ترکیب لازم است، چون معیارهای مستقل از آستانه و وابسته به آستانه سؤال‌های متفاوتی را پاسخ می‌دهند.

در ارزیابی فدرال، باید دقت نهایی، میانگین ۱۰ دور پایانی، سرعت همگرایی، واریانس بین کلاینت‌ها، نسبت کلاینت‌های منتخب، و هزینه ارتباطی گزارش شوند. کارایی نیز باید با زمان اجرا، بایت‌های منتقل‌شده، و دقت به‌ازای هر مگابایت سنجیده شود.

۶ نتایج و بحث

نتایج باید بر پایه هفت آزمایش فوق سازمان‌دهی شوند، نه بر مبنای جزئیات پیاده‌سازی. E1 باید نشان دهد که مدل اصلی دقت مجموعه بسته را حفظ می‌کند. E2 باید ارزش واسنجی EVT را برای رد حملات ناشناخته جدا کند. E3 باید FedAvg، FedProx، و FMRL-LA را تحت ناهمگنی فزاینده مقایسه کند. E4 باید هم‌زمانیِ فدرال غیرهمسان و رد مجموعه‌باز را بسنجد. E5 باید سهم EVT، مولد، و تجمیع آگاه از سودمندی را جدا کند. E6 باید هزینه مکانیزم دو فازه را کمی‌سازی کند. E7 باید نشان دهد که جداسازی مجموعه‌باز برای برچسب‌های مختلف سازگار است.

بحث باید صریحاً دادوستدها را تفسیر کند. برای مثال، اگر FMRL-

جدول ۲: ماتریس آزمایش‌های نهایی

آزمایش	هدف	خروجی اصلی
E1	اعتبارسنجی مجموعه بسته	دقت، macro F1، دقت متوازن
E2	تشخیص مجموعه‌باز	AUROC، AUPRC، FPR@95%TPR، un-known F1
E3	فدرال غیرهمسان	پایداری، همگرایی، هزینه ارتباطی
E4	آزمون هم‌زمان	معیارهای شناخته‌شده و ناشناخته تحت ناهمگنی
E5	حذف مؤلفه و حساسیت	افت معیار و پایداری آستانه
E6	کارایی و مقیاس‌پذیری	زمان اجرا، بایت‌های منتقل‌شده، دور تا همگرایی
E7	آزمون برچسب‌محور	جداسازی در فضای نهفته و ردِ هر برچسب

LA پایداری را بهبود دهد اما هماهنگی بیشتری بخواهد، این بده‌بستان باید با نمودار هزینه ارتباطی و نمودار دقت دوربه‌دور نشان داده شود. اگر EVT تشخیص ناشناخته را بهتر کند ولی کمی دقت کلاس‌های شناخته‌شده را نزدیک آستانه کاهش دهد، منحنی کالیبراسیون باید آن را آشکار کند.

۷ حذف مؤلفه

حذف مؤلفه‌ها باید شامل حذف رد EVT، حذف آموزش مولد، جایگزینی FMRL-LA با FedAvg، جایگزینی FMRL-LA با FedProx، و غیرفعال‌سازی انتخاب کلاینت باشد. تحلیل حساسیت نیز باید α دایریکله، کسر دم EVT، آستانه سودمندی، و بذرهای تصادفی را بررسی کند. این نتایج ارزش هر زیرسامانه و میزان پایداری روش را روشن می‌کنند.

۸ محدودیت‌ها و اعتبارسنجی

محدودیت‌های اصلی شامل حساسیت کالیبراسیون، هزینه هماهنگی دو مرحله‌ای، و تمرکز فعلی بر B-NAT به‌جای چند مجموعه‌داده بیرونی است. کیفیت EVT به تقسیم اعتبارسنجی وابسته است و FMRL-LA به وضعیت سمت سرور و پایش اضافی نیاز دارد. این محدودیت‌ها باید صریحاً ذکر شوند تا مقاله بیش از حد کلی‌گرا به نظر نرسد.

۹ بازتولیدپذیری

مخزن، پیکربندی Hydra، کنترل بذر، ذخیره‌سازی checkpoint، خروجی محلی، و نمودارهای سطح اجرا را فراهم می‌کند. این ویژگی‌ها خط لوله را در مراحل پیش‌پردازش، آموزش، ارزیابی، و تولید شکل‌ها بازتولیدپذیر می‌سازند. نسخه نهایی مقاله باید به خروجی‌های ذخیره‌شده و قرارداد ارزیابی ثابت ارجاع دهد تا نتایج از همان تقسیم و همان فهرست بذرها قابل بازسازی باشند.

۱۰ جمع‌بندی

CF-MARLOS یک چارچوب یکپارچه برای تشخیص نفوذ مجموعه‌باز در محیط‌های فدرال و غیرهمسان ارائه می‌دهد. این روش با ترکیب یادگیری محلی CVAE-DQN، تجمیع فدرال، بازسازی مبتنی بر مولد، و واسنجی EVT، برای حفظ دقت کلاس‌های شناخته‌شده، رد حملات ناشناخته، و پایداری تحت قطعات غیرهمسان طراحی شده است. بخش تجربی نهایی باید این ادعاها را با بودجه یکسان و مقایسه‌های کنترل‌شده نشان دهد.

References

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of AISTATS*, pages 1273–1282, 2017.

[2] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith. Federated optimization in heterogeneous networks. In *Proceedings of MLSys*, 2020.

[3] H. van Hasselt, A. Guez, and D. Silver. Deep reinforcement learning with double Q-learning. In *Proceedings of AAAI*, 2016.

[4] A. Bendale and T. E. Boult. Towards open set deep networks. In *Proceedings of CVPR*, pages 1563–1572, 2016.

[5] E. M. Rudd, L. P. Jain, W. J. Scheirer, and T. E. Boult. The extreme value machine. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(3):762–768, 2018.