جلسه دفاع پایان نامه کارشناسی ارشد
مهندسی کامپیوتر-شبکه های کامپیوتری

عنوان

بهبود دقت تشخیص نفوذ به کمک یادگیری عمیق با الگوریتم بهینه Adam و تابع فعالساز LEAKY RELU

استاد راهنما: آقای دکتر سید رضا کامل

دانشجو: مریم مهدوی

شهریور 1401

فهرست مطالب

مقدمه

بیان مساله پژوهش

اهمیت و هدف و جنبه های نوآوری پژوهش

فرضیات پزوهش

مختصری بر روش تحقیق

مرور ادبیات

سیستم های تشخیص نفوذ

یادگیری عمیق

اصطلاحات رایج

کارای پیشین

روش پیشنهادی

الگوریتم روش پیشنهادی

جزئیات روش پیشنهادی

تحلیل و ارزیابی

جزئیات روش ارزیابی

تحلیل نتایج ارزیابی

نتیجه گیری

بیان مساله | اهداف تحقیق | اهمیت موضوع | نوآوری تحقیق

فرضیه تحقیق | روش تحقیق

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

بیان مساله

نفوذ در شبکه‌های کامپیوتری با هدف‌های متفاوتی از جمله سیاسی، مالی، نظامی و یا نمایان کردن سستی‌های امنیتی موجود در برنامه‌های کاربردی صورت می‌گیرد.

داده‌کاوی و یادگیری ماشین از راه‌های حیاتی یافتن علم سودمند اطلاعات در داده‌ها می‌باشد که در تحلیل انواع شبکه ها کاربرد دارد.

مهم‌ترین مساله و چالشی که در این روش‌ها وجود دارد جداسازی فعالیت‌های نرمال از حملات است.

برای بهبود دقت در این شبکه از پروسپترون چندلایه استفاده می کنیم.

مریم مهدوی

بیان مساله | اهداف تحقیق | اهمیت موضوع | نوآوری تحقیق

فرضیه تحقیق | روش تحقیق

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

اهداف

به طور کلی ما به دنبال راهی جهت بهبود دقت در سیستم های تشخیص نفوذ می باشیم

اهمیت

با افزایش روز افزون حملات به سیستم ها و اهمیت صحت و درستی داده ها در حوزه های مختلف روش های مقابله بسیار مهم می باشد

نوآوری

نوآوری این پژوهش برای حل مسأله دقت افزایش لایه های شبکه پروسپترن که یکی از روش های یادگیری عمیق می‌باشد و استفاده از الگوریتم adamو تابع فعالساز leaky relu در طراحی این شبکه است.

مریم مهدوی

بیان مساله | اهداف تحقیق | اهمیت موضوع | نوآوری تحقیق

فرضیه تحقیق | روش تحقیق

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

فرضیه

با افزایش تعدادلایه های mlp و استفاده از تابع فعالساز leaky relu و الگوریتم بهینه adam میتوان بهبود دردقت تشخیص فعالیت های نرمال از حمله انجام داد.

مریم مهدوی

بیان مساله | اهداف تحقیق | اهمیت موضوع | نوآوری تحقیق

فرضیه تحقیق | روش تحقیق

روش

در ابتدا مجموعه داده NSL-KDD را با تحلیل مولفه‌های اساسی(PCA) که یکی از روش‌های کاهش ویژگی از طریق استخراج ویژگی می‌باشد، کاهش ابعاد می‌دهیم و در مرحله بعدی مجموعه داده را به شبکه پروسپترون چهار لایه که از الگوریتم Adam جهت به‌روزسانی وزن‌ها و استفاده از تابع فعالساز Leaky relu در لایه اول، دوم و سوم طراحی کرده‌ایم تزریق می کنیم و در نهایت دقت را بررسی می کنیم

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

سیستم های تشخیص نفوذ

سیستم تشخیص نفوذ (IDS[1]): وظیفه شناسایی و تشخیص هر گونه استفاده غیرمجاز از سیستم و سواستفاده یا آسیب رسانی توسط هر دو دسته کاربران داخلی و خارجی را بر عهده دارند.

هدف سیستم‌های تشخیص نفوذ را می‌توان به صورت زیر خلاصه کرد:

- ✓ امکان برقراری ارتباط بین یک واقعه و شخص مسئول آن واقعه
- ✓ امکان شناسایی حمله و واکنش قابل قبول برای مقابله یا توقف آن و جلوگیری از تکرار حمله
- ✓ فرایند تولید، ثبت و مرور یک سابقه از عملکرد سیستم

به‌طورکلی روش‌های تشخیص نفوذ در میزبان و شبکه به دو دسته مبتنی بر سوءاستفاده یا امضاء و روش مبتنی بر ناهنجاری طبقه‌بندی می‌شود.

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

یادگیری ماشین که زیرمجموعه‌های از هوش مصنوعی است، رایانه را به‌گونه‌ای توانمند می‌سازد که قادر به یادگیری از طریق تجربه و بدون برنامه‌ریزی صریح می‌شود.

هوش مصنوعی ترکیب هوش انسانی در ماشین است، به‌نحوی که رفتاری همانند انسان را تقلید و خلاقانه مسائل را حل کند.

یادگیری عمیق زیرمجموعه‌ای از یادگیری ماشین بوده و از ساختار شبکه‌های عصبی برای تقلید در تصمیم‌گیری حل یک مسئله مشابه مغز انسان استفاده می‌کند

مقدمه

مرور ادبیات

روش پیشنهادی

تحلیل و ارزیابی

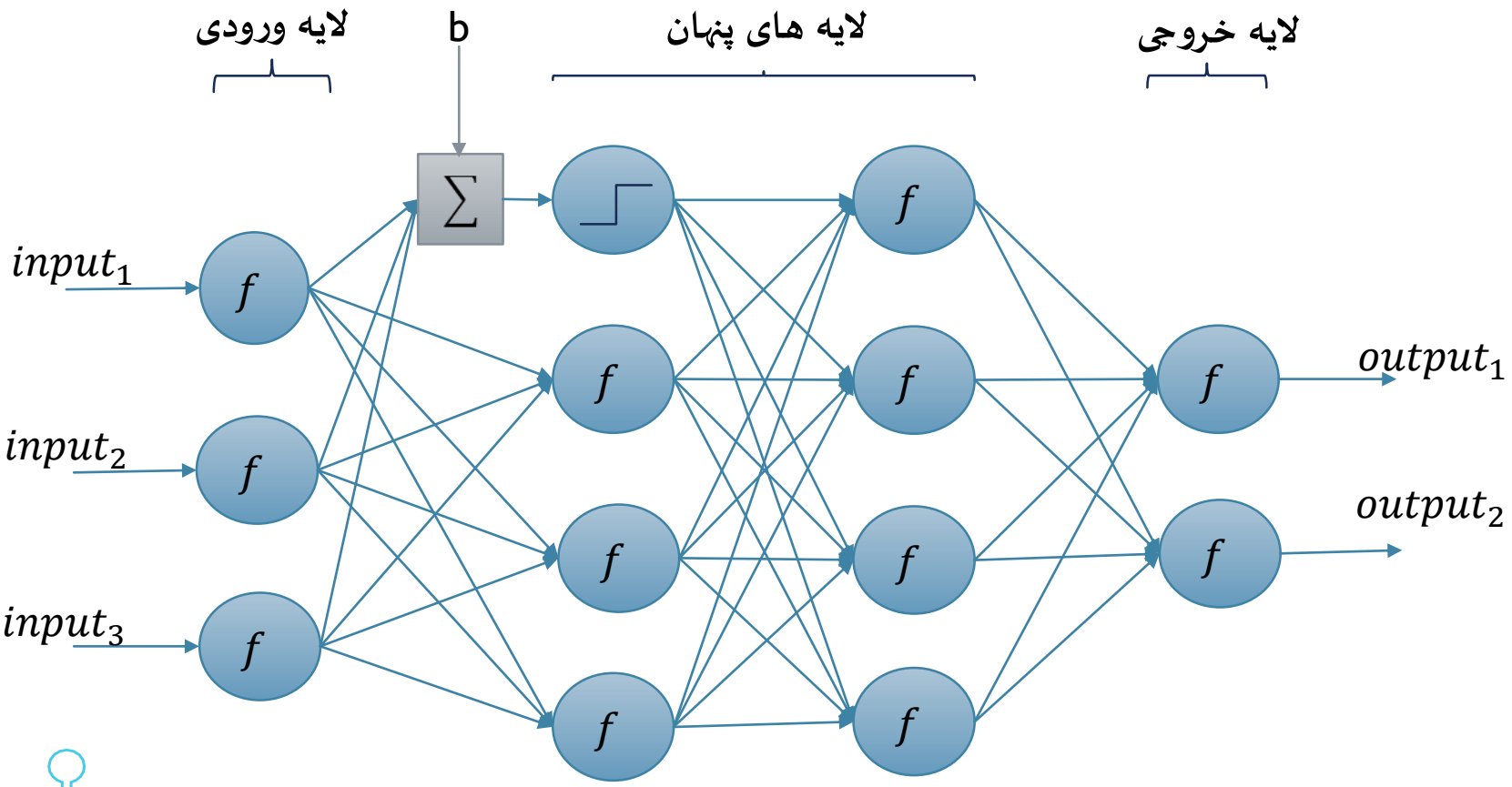
نتیجه گیری

شبکه های عصبی

شبکه‌های عصبی مصنوعی مدل‌های محاسباتی بوده که سازوکار یادگیری را همانند شبکه عصبی طبیعی از ساختار مغز انسان شبیه‌سازی می‌کند.
شبکه های پروپسترون چندلایه (MLP):دسته ای از شبکه عصبی نظارت شده است.
نگاه مدرن به شبکه های عصبی در دهه 1940 و با شروع به کار McCulloch و Pitts آغاز شد، علاقه به شبکه های عصبی را اواخر دهه 1960 به خاطر کمبود کامپیوترهای قدرتمند و ایده های جدید دچار وقفه شد و در طول 1980 هردوی این موانع برداشته شد و تحقیقات در این زمینه جان تازه ای گرفت و در زمان حال حاضر بسیار مورد توجه محقیق قرار گرفته است

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

معماری و ساختار شبکه



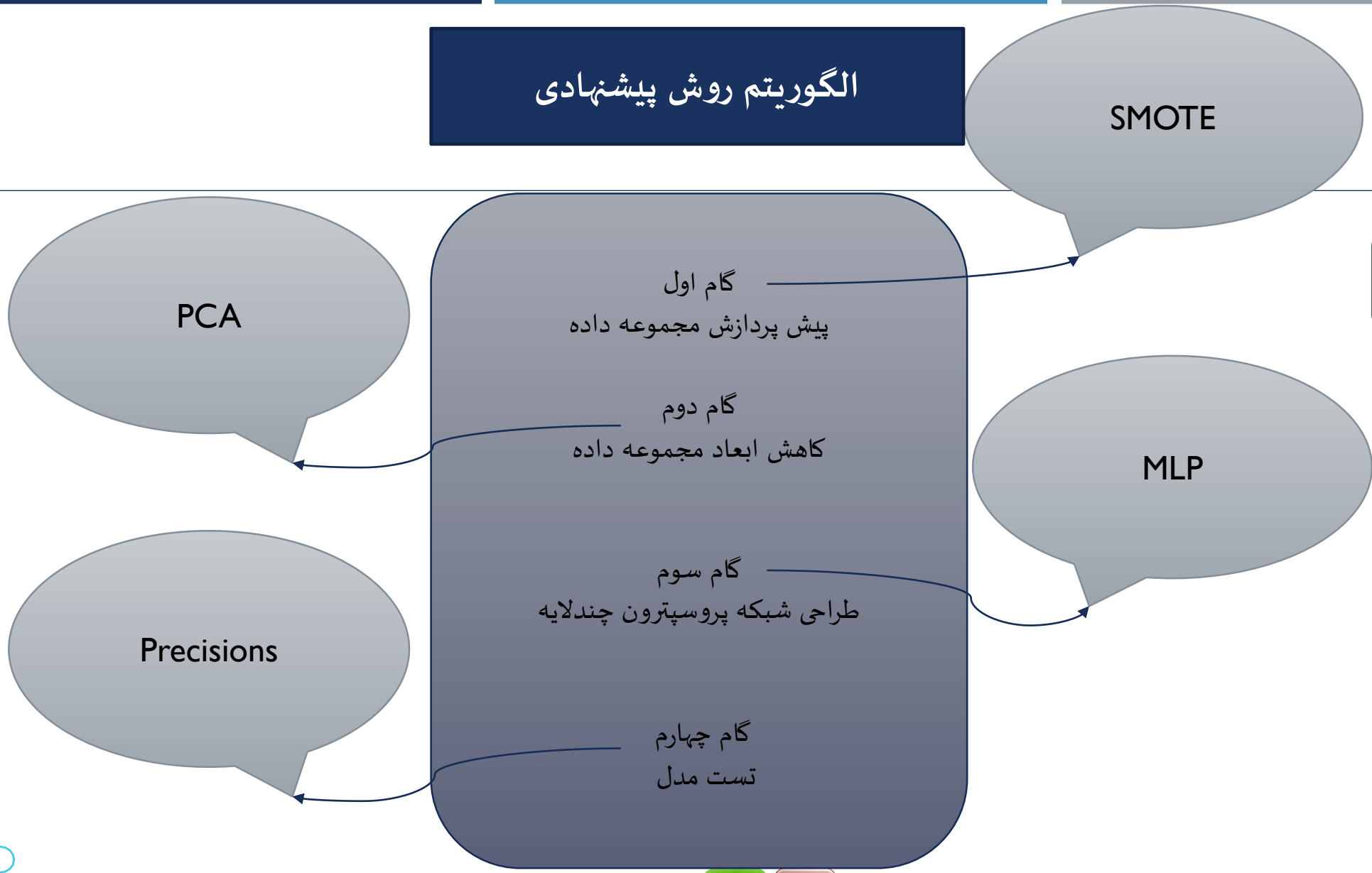
مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری
mlp
انواع لایه ها
نرون
بایاس
وزن
توابع فعالساز
روش های یادگیری
تابع هزینه
الگوریتم بهینه سازی
دوره
نرخ یادگیری
معیار عملکرد

مریم مهدوی

کارهای پیشین

ردیف	سال-تحقیق	روش انجام پژوهش	مجموعه داده
۱	[۷]-۲۰۲۱	الگوریتم ترکیبی مبتنی برK-MEANS توزیع‌شده، RF و یادگیری عمیق	NSL-KDD CIC-IDS2017
۲	[۵]-۲۰۲۰	الگوریتم PCA-DL: تجزیه‌وتحلیل مولفه‌های اصلی با یادگیری عمیق	NSL-KDD
۳	[۶]-۲۰۲۰	الگوریتم FSL: یادگیری مجموعه‌داده محدود	NSL-KDD UNSW-NB15
۴	[۳۰]-۲۰۲۰	الگوریتم DLS-IDS : تشخیص نفوذ با جرقه یادگیری عمیق	NSL-KDD
۵	[۸]-۲۰۱۹	الگوریتم FFDNN: مبتنی بر یادگیری عمیق و شبکه‌های عصبی عمیق	NSL-KDD
۶	[۹]-۲۰۱۹	الگوریتم ترکیبی با مدل یادگیری عمیق و شبکه‌های عصبی عمیق	NSL-KDD KDDCUP99 UNSW-NB15 WSN-DS
۷	[۱۱]-۲۰۱۸	الگوریتم GRU: مبتنی یر شبکه‌های عصبی عمیق با واحدهای مکرر	NSL-KDD KDD 99
۸	[۱۲]-۲۰۱۸	الگوریتم STL: مبتنی بر خودرمزگذار	NSL-KDD
۹	[۱۳]-۲۰۱۸	الگوریتم SSAE: رمزگذار خودکار پراکنده	NSL-KDD
۱۰	[۲۷]-۲۰۱۸	الگوریتم IG-PCA: رویکرد کسب اطلاعات با تجزیه و تحلیل مولفه‌های اصلی	ISCX 2012 NSL-KDD +KYOTO 2006

الگوریتم روش پیشنهادی



مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

جزئیات الگوریتم روش پیشنهادی

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

به طور کلی برای پیاده سازی روش پیشنهادی در چهار بخش تکمیل می شود

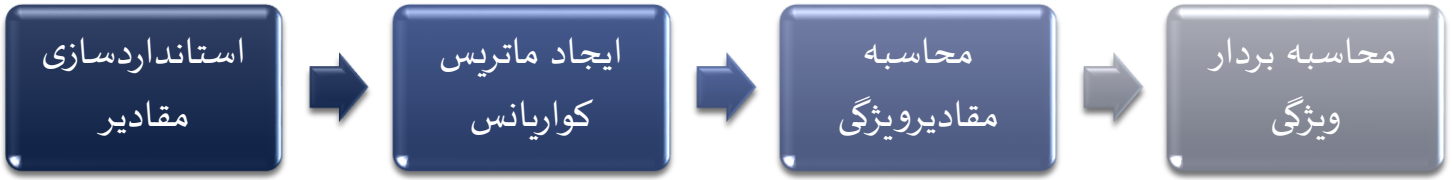
بخش اول

درابتدا برای رفع مشکل نامتعادل بودن کلاس‌های مجموعه‌داده از روش Smote برای متعادل‌سازی استفاده می‌کنیم.

بخش دوم

با الگوریتم تجزیه و تحلیل مولفه‌های اصلی (PCA)کار کاهش بعد را برای افزایش بهبود سرعت پردازش داده‌ها صورت می‌گیرد که در چهار مرحله صورت می گیرد

.



جزئیات الگوریتم روش پیشنهادی

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

بخش سوم

در بخش سوم ساختار شبکه mlp را طراحی می کنیم

معماری شبکه عصبی شامل چهار لایه می باشد

- یک لایه ورودی: که در آن از تابع فعالساز leaky relu استفاده شده است
- دو لایه پنهان: که در آن از تابع فعالساز leaky relu استفاده شده است
- لایه خروجی: که از تابع فعالساز softmax استفاده شده است

تعدادی از مقادیر که با عنوان فراپارامترها می شناسیم در این مرحله مشخص می شود این مقادیر شامل تابع فعال ساز، تعداد نرون ها در هر لایه، مقداردهی اولیه، الگوریتم بهینه سازی و نرخ یادگیری، تعداد دوره، تابع ضرر است. در ادامه به توضیح دو فراپارامتر تابع فعالساز و الگوریتم بهینه می پردازیم

جزئیات الگوریتم روش پیشنهادی

تابع یکسوساز خطی رخنه‌دار(Leaky relu): این تابع فعالسازی مشکل مرگ نرون‌ها در طول فرایند آموزش را ازبین می‌برد.برای افزایش سرعت مدل می‌توان از این تابع در لایه ورودی ودو لایه پنهان استفاده کرد.

$$LeakyRelu = \begin{cases} x & x \geq \text{اگر: صفر} \\ ax & x < \text{اگر: صفر} \end{cases}$$

بهینه سازها و به هنگام سازی وزن ها: الگوریتم‌هایی هستند که به واسطه به‌روزرسانی وزن‌ها در شبکه تلاش در جهت کم کردن تابع ضرر دارد. الگوریتم Adamاز سایر روش‌های تطبیقی بهتر عمل می‌کند و خیلی سریع همگرا می‌شود. همچنین بر سایر مشکلاتی که الگوریتم‌های بهینه‌سازی همانند فروپاشی نرخ یادگیری، واریانس بالا در به‌هنگام‌سازی و همگرایی آهسته دارند، غلبه می‌کندبرای بهینه کردن مقدار وزن‌ها و بایاس در این پژوهش از الگوریتم Adam استفاده می‌شود.

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

جزئیات الگوریتم روش پیشنهادی

Require: α: Stepsize
Require: $\beta_1, \beta_2 \in [0, 1)$: Exponential decay rates for the moment estimates
Require: $f(\theta)$: Stochastic objective function with parameters θ
Require: θ_0: Initial parameter vector
$m_0 \leftarrow 0$ (Initialize 1^{st} moment vector)
$v_0 \leftarrow 0$ (Initialize 2^{nd} moment vector)
$t \leftarrow 0$ (Initialize timestep)
while θ_t not converged **do**
$t \leftarrow t + 1$
$g_t \leftarrow \nabla_\theta f_t(\theta_{t-1})$ (Get gradients w.r.t. stochastic objective at timestep t)
$m_t \leftarrow \beta_1 \cdot m_{t-1} + (1 - \beta_1) \cdot g_t$ (Update biased first moment estimate)
$v_t \leftarrow \beta_2 \cdot v_{t-1} + (1 - \beta_2) \cdot g_t^2$ (Update biased second raw moment estimate)
$\widehat{m}_t \leftarrow m_t / (1 - \beta_1^t)$ (Compute bias-corrected first moment estimate)
$\widehat{v}_t \leftarrow v_t / (1 - \beta_2^t)$ (Compute bias-corrected second raw moment estimate)
$\theta_t \leftarrow \theta_{t-1} - \alpha \cdot \widehat{m}_t / (\sqrt{\widehat{v}_t} + \epsilon)$ (Update parameters)
end while
return θ_t (Resulting parameters)

بخش چهارم

در این بخش مدلسازی صورت گرفته است و با مجموعه داده آزمایشی برنامه را اجرا می‌کنیم و دقت را بدست می‌آوریم.

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

روش ارزیابی

مجموعه‌داده NSL-KDD که شامل ۴۱ ویژگی و۱۶۰۳۱۷ رکورد است.
این مجموعه‌داده شامل پنج کلاس است که یک کلاس نرمال و چهار کلاس حمله PROB DOS,R2L,U2R, است.

.

دسته‌بندی داده‌ها	چند کلاسه				
	نرمال	Dos	Probe	R2L	U2R
آموزشی	۶۷۳۴۳	۴۵۹۲۷	۱۱۶۵۶	۹۹۲	۵۲
آزمایشی	۹۷۱۱	۷۴۵۸	۲۴۲۱	۲۷۵۴	۲۰۰
کل	۷۷۰۵۴	۵۳۳۸۵	۱۴۰۷۷	۳۷۴۶	۲۵۲

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

روش ارزیابی

قسمتی از مجموعه دادهNSL-KDD

```
0,tcp,ftp_data,SF,491,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,0.00,0.00,1.00,0.00,0.00,150,25,0.17,
0,udp,other,SF,146,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,13,1,0.00,0.00,0.00,0.00,0.08,0.15,0.00,255,1,0.00,0.6
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,123,6,1.00,1.00,0.00,0.00,0.05,0.07,0.00,255,26,0.10,0
0,tcp,http,SF,232,8153,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,5,5,0.20,0.20,0.00,0.00,1.00,0.00,0.00,30,255,1.00,0
0,tcp,http,SF,199,420,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,30,32,0.00,0.00,0.00,0.00,1.00,0.00,0.09,255,255,1.00
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,121,19,0.00,0.00,1.00,1.00,0.16,0.06,0.00,255,19,0.07
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,166,9,1.00,1.00,0.00,0.00,0.05,0.06,0.00,255,9,0.04,0.
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,117,16,1.00,1.00,0.00,0.00,0.14,0.06,0.00,255,15,0.06,
0,tcp,remote_job,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,270,23,1.00,1.00,0.00,0.00,0.09,0.05,0.00,255,23,0.
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,133,8,1.00,1.00,0.00,0.00,0.06,0.06,0.00,255,13,0.05,0
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,205,12,0.00,0.00,1.00,1.00,0.06,0.06,0.00,255,12,0.05
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,199,3,1.00,1.00,0.00,0.00,0.02,0.06,0.00,255,13,0.05,0
0,tcp,http,SF,287,2251,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,3,7,0.00,0.00,0.00,0.00,1.00,0.00,0.43,8,219,1.00,0.
0,tcp,ftp_data,SF,334,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,2,2,0.00,0.00,0.00,0.00,1.00,0.00,0.00,2,20,1.00,0.
0,tcp,name,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,233,1,1.00,1.00,0.00,0.00,0.00,0.06,0.00,255,1,0.00,0.07,
0,tcp,netbios_ns,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,96,16,1.00,1.00,0.00,0.00,0.17,0.05,0.00,255,2,0.01
0,tcp,http,SF,300,13788,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,8,9,0.00,0.11,0.00,0.00,1.00,0.00,0.22,91,255,1.00,
0,icmp,eco_i,SF,18,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,1,16,1.00,0.00,
0,tcp,http,SF,233,616,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,3,3,0.00,0.00,0.00,0.00,1.00,0.00,0.00,66,255,1.00,0.
0,tcp,http,SF,343,1178,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,9,10,0.00,0.00,0.00,0.00,1.00,0.00,0.20,157,255,1.00
0,tcp,mtp,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,223,23,1.00,1.00,0.00,0.00,0.10,0.05,0.00,255,23,0.09,0.05
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,280,17,1.00,1.00,0.00,0.00,0.06,0.05,0.00,238,17,0.07,
0,tcp,http,SF,253,11905,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,8,10,0.00,0.00,0.00,0.00,1.00,0.00,0.20,87,255,1.00
```


مقدمه

مرور ادبیات

روش پیشنهادی

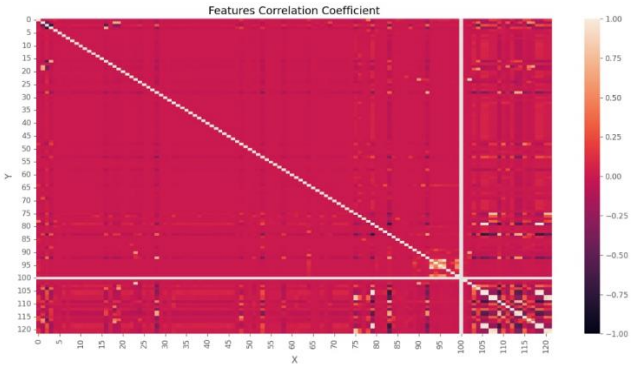
تحلیل و ارزیابی

نتیجه گیری

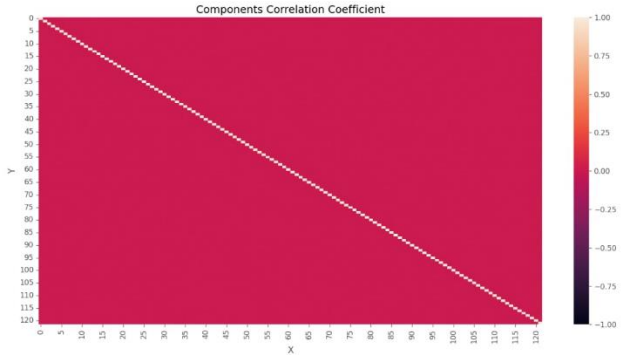
روش ارزیابی

PCA: طی فرآیند کاهش ابعاد در مجموعه داده NSL-KDD می‌توان گفت PCA مواردی را به دنبال دارد از جمله:

- چگونگی ارتباط هر یک از متغییرها با یگدیگر به وسیله ایجاد ماتریس کوواریانس می‌توان پی برد.
- داده‌ها در چه جهاتی پراکنده هستند از طریق بردار ویژگی بدست می‌آید.
- مقدار اهمیت هریک از جهات‌ها که با مقادیر ویژه مشخص می‌شود
- در شکل الف و ب میزان همبستگی بین ویژگی در حالت بدون اعمال PCA و با اعمال PCA نمایش داده شده است.



الف)بدون اعمال PCA



ب)با اعمال PCA

روش ارزیابی

طراحی شبکهMLP: جهت اجرای دقیق شبکه در محیط برنامه‌نویسی پایتون با پردازنده xeon2coreو ROM 8صورت می‌گیرد و تنظیمات ابرپارامترها در شبکه عصبی عمیق به صورت زیر است

نوع ابرپارامتر	مقدار
تعداد لایه	4
تعداد نرون درلایه اول	84
تعداد نرون درلایه دوم	256
تعداد نرون درلایه سوم	128
تعداد نرون درلایه چهارم	5
توابع فعالساز	Leaky relu,softmax
تابع زیان	cross entropy
الگوریتم بهینه‌سازی	adam
وزن‌دهی اولیه	مقداردهی اولیه یکنواخت گلوروت
دوره	10
اندازه دسته	32
نرخ یادگیری	0.0003

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

به اختلاف بین مقدار بدست‌آمده از مدل و مقدار واقعی خطا می‌گوییم

نام الگوریتم	خطا
الگوریتم PCA-DL	0.057
الگوریتم پیشنهادی	0.055

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

تعداد پیش‌بینی‌های درست بازگردانده‌شده توسط مدل را می‌توان با صحت عنوان کرد

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

نام الگوریتم	صحت
الگوریتمPCA-DL	96 درصد
الگوریتم پیشنهادی	98 درصد

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

تعداد مثبت‌های برگردانده‌شده توسط مدل را می‌توان با عنوان یادآور(recall) یا حساسیت(sensitivity) نام برد

$$Recall = \frac{TP}{TP + FN}$$

نام الگوریتم	یادآوری
الگوریتم PCA-DL	93 درصد
الگوریتم پیشنهادی	93 درصد

تعداد مقادیر صحیح برگردانندهشده توسط مدل را می‌توان دقت نام برد

$$Precisions = \frac{TP}{TP + FP}$$

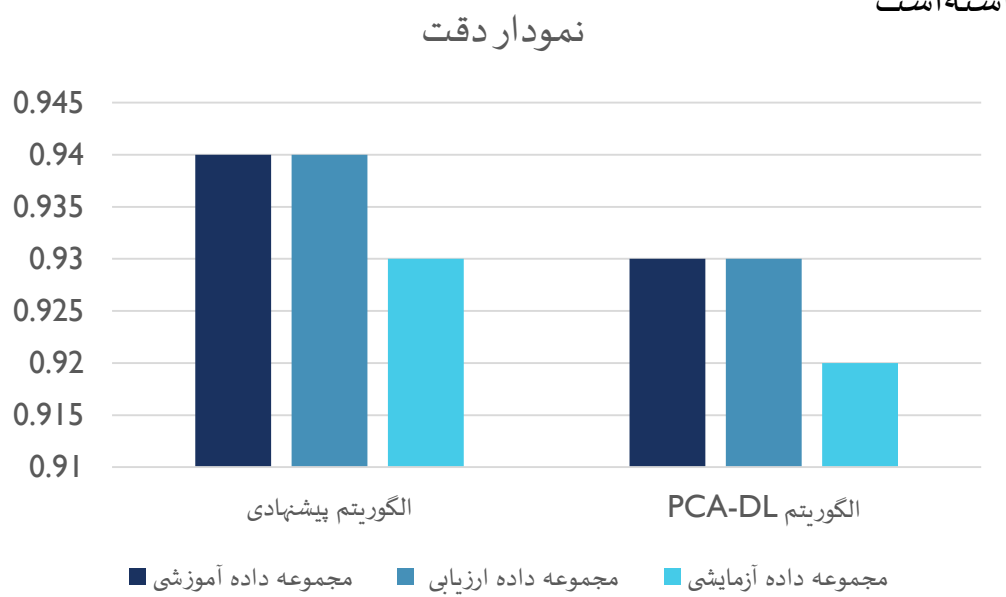
نام الگوریتم	دقت
الگوریتمPCA-DL	92 درصد
الگوریتم پیشنهادی	93 درصد

این زمان شامل زمان محاسبه مجموعه داده آموزش و آزمایش مدل می‌باشد

نام الگوریتم	زمان محاسباتی
الگوریتم PCA-DL	18s 12ms
الگوریتم پیشنهادی	26s 18ms

مقدمه
مرور ادبیات
روش پیشنهادی
تحلیل و ارزیابی
نتیجه گیری

ما روش پیشنهادی را به همراه تحلیل مولفه‌های اساسی و شبکه پروسپترون چهار لایه در محیط برنامه‌نویسی python اجرا کرده ایم با مقایسه نتایج پیاده‌سازی می‌توان دریافت که روش پیشنهادی با افزایش لایه‌های پنهان که کار پردازش را انجام‌می‌دهد توانستیم دقت تشخیص نفوذ را به 93 درصد افزایش دهیم .این بهبود دقت نشان می‌دهد که روش پیشنهادی در مقایسه با الگوریتم pca-dlعملکرد بهتری در رسیدن به افزایش دقت سیستم‌های تشخیص نفوذ داشته‌است



منابع

[1] M. Haggag, M. M. Tantawy, and M. M. S. El-Soudani, "Implementing a deep learning model for intrusion detection on apache spark platform," *IEEE Access*, vol. 8, no. DI, pp. 163660–163672, 2020, doi: 10.1109/ACCESS.2020.3019931.

[2] S. Sunita, B. J. Chandrakanta, and R. Chinmayee, "A Hybrid Approach of Intrusion Detection using ANN and FCM," *Eur. J. Adv. Eng. Technol.*, vol. 3, no. 2, pp. 6–14, 2016.

[3] H. Rajadurai and U. D. Gandhi, "An empirical model in intrusion detection systems using principal component analysis and deep learning models," *Comput. Intell.*, vol. 37, no. 3, pp. 1111–1124, 2021, doi: 10.1111/coin.12342.

[4] Y. Yu and N. Bian, "An Intrusion Detection Method Using Few-Shot Learning," *IEEE Access*, vol. 8, no. 1, pp. 49730–49740, 2020, doi: 10.1109/ACCESS.2020.2980136.

[5] C. Liu, Z. Gu, and J. Wang, "A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning," *IEEE Access*, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[6] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[7] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[8] B. Singh and A. Kr Ahlawat, "Innovative Empirical Approach for Intrusion Detection Using ANN," *Int. J. Innov. Res. Comput. Sci. Technol.*, no. 4, pp. 2347–5552, 2016.

[9] C. Xu, J. Shen, X. Du, and F. Zhang, "An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[10] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.

[11] B. Yan and G. Han, "Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System," *IEEE Access*, vol. 6, pp. 41238–41248, 2018, doi: 10.1109/ACCESS.2018.2858277.

[12] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Comput. Networks*, vol. 148, no. November, pp. 164–175, 2019, doi: 10.1016/j.comnet.2018.11.010.

سپاس از توجه شما

Maryammahdavi.sh72@gmail.com