سیستم‌های فازی و کاربردها
سال سوم، شماره اول (بهار و تابستان ۱۳۹۹) صص. ۶۳ تا ۷۴
DOR: 20.1001.1.27174409.1399.3.1.4.9

طراحی یک سیستم تشخیص نفوذ به کمک روش های مبتنی برسیستم های هوشمند

میثم ثمره قاسم، مرجان کوچکی رفسنجانی *

گروه علوم کامپیوتر، دانشگاه شهید باهنر کرمان، کرمان، ایران

چکیده

بشر در حال گذران برهه ای از تاریخ خود است که سیستم های کامپیوتری به بخشی جدایی ناپذیر از حیات وی بدل شده است. سیستم های کامپیوتری و به طور خاص شبکه‌های کامپیوتری در بسیاری از جنبه‌های زندگی امروزی نقش تعیین کننده‌ای داشته و به همین دلیل امنیت آن‌ها بسیار مورد توجه است. برای پوشش امنیت آن‌ها و در اصطلاح تشخیص نفوذ در یک شبکه کامپیوتری روش‌های زیادی از جمله شبکه‌های عصبی مصنوعی پیشنهاد شده است، اما یکی از چالش‌های شبکه‌های عصبی افتادن در دام بهینه‌های محلی است. از دلایل بروز این مشکل استفاده از روش های مبتنی بر کاهش شیب در فرآیند آموزش است که در نتیجه برای حل این چالش از روش‌های بهینه سازی بسیاری استفاده می شود. در این مقاله سعی شده است با استفاده از الگوریتم رقابت استعماری یک شبکه عصبی پرسپترون چند لایه را آموزش داده و به منظور بررسی کارایی آن، روش پیشنهادی با دو روش دیگر مقایسه شده است. نتایج روش پیشنهادی در مواردی که تعداد نمونه ها بیشتر بوده است بهبود ۱۰ تا ۱۵ درصدی را به دنبال داشته است.

Mathematics Subject Classification (2010): 68M10 ; 78M32 , **Email:** Kuchaki@uk.ac.ir.

عبارات و کلمات کلیدی:سیستم‌های تشخیص نفوذ، شبکه عصبی پرسپترون چند لایه، الگوریتم رقابت استعماری

۱۳۹۹ (انجمن سیستم‌های فازی ایران)

۱ سرآغاز

امروزه شبکه‌های کامپیوتری به بخشی جداناپذیر زندگی بشری تبدیل شده‌اند. شبکه‌های کامپیوتری فقط به کامپیوترها محدود نبوده و شامل گوشی‌های هوشمند، تبلت‌ها و سایر ارتباطات شبکه‌ای هم می‌شود. همچنان که استفاده از شبکه‌های کامپیوتری فراگیرتر می‌شود، میزان حملات به آن‌ها نیز افزایش یافته و بنابراین توجه به امنیت ضروری‌تر می‌شود. نفوذ یکی از اقدامات مهاجمان برای خدشه در امنیت شبکه‌های کامپیوتری است. نفوذ عبارت است از: دسترسی به اطلاعات بدون تغییری در آن‌ها، تغییر یا دستکاری اطلاعات، از دسترس خارج شدن سیستم (شبکه) به طور خلاصه به هر اقدامی که پارامترهای یک شبکه امن را نقض کند نفوذ گفته می‌شود [۱، ۶، ۷]. یک سیستم تشخیص نفوذ[1] نرم افزاری است با یک تابع محاسباتی آشکارساز که فعالیت‌های غیرطبیعی[2] و مضر را تشخیص و به بخش تعریف شده‌ای از شبکه گزارش می‌کند [۱۵، ۲۰]. در این سیستم‌ها، تشخیص به سه دسته کلی زیر تقسیم می‌شود: ناهنجاری[3]، سوءاستفاده[4] و ترکیبی از سوءاستفاده و ناهنجاری. در تشخیص ناهنجاری یک پایگاه داده از رفتارهای مجاز وجود داشته و هر اقدامی که مطابق این پایگاه داده نباشد کاندیدای رفتاری مضر و مخرب است. اما در تشخیص سوءاستفاده ابتدا الگویی از رفتارهای غیرطبیعی تشکیل شده و رفتارهای آینده براساس این الگو طبقه بندی می‌شوند [۵، ۱۰، ۱۱، ۱۵]. برای پوشش امنیت شبکه‌های کامپیوتری روش‌هایی از دیرباز مطرح شده‌اند که به دو دسته روش‌های قدیمی و نوین تقسیم می‌شوند. روش‌هایی مانند دیواره آتش[5]، تایید هویت کاربر[6]، رمزگذاری داده‌ها[7]، کنترل جریان دسترسی[8] و ... از جمله روش‌هایی هستند که در دسته‌بندی قدیم ارزیابی می‌شوند. اما این روش‌ها هر کدام به دلایلی در برخی حملات کارایی لازم را ندارند [۵، ۱۰، ۱۱، ۱۵، ۲۰، ۲۴].

[1] Intrusion Detection System (IDS)
[2] Abnormal
[3] Anomaly
[4] Misuse
[5] Firewall
[6] User authentication
[7] Data encryption
[8] Access control scheme

بنابراین بسیاری از تحقیقات بر استفاده از روش‌های نوینی همچون استفاده از روش‌های مبتنی بر هوش مصنوعی[9] و یا روش های طبقه بندی براساس قوانین آماری متمرکز شده‌اند. در بعضی از تحقیقات از شبکه‌های عصبی پرسپترون چند لایه[10] [۹، ۱۲، ۲۵]، شبکه‌های عصبی شعاع مبنا[11] [۹، ۱۸] به عنوان IDS استفاده شده است. همچنین برخی پژوهش‌ها از ماشین‌های بردار پشتیبان[12] [۲، ۱۳، ۱۷]، درخت تصمیم[13] [۱۶، ۲۱] و یا ترکیبی از چند روش هوشمند [۳، ۱۶، ۲۳] استفاده کرده‌اند. شبکه‌های عصبی مصنوعی به عنوان یک یادگیرنده قوی مسائلی سخت در علوم مختلف را با دقتی خوب حل کرده است. با این وجود یکی از ضعف‌های این روش‌ها افتادن در بهینه محلی است. این مشکل ناشی از الگوریتم یادگیری آن‌هاست که مبتنی بر کاهش شیب[14] عمل می‌کند. در فرآیند یادگیری یک شبکه عصبی الگوریتم یادگیری تلاش دارد با تنظیم مقادیر وزن‌هاو بایاس‌هاعملکرد شبکه عصبی بهتر شود. به بیان دیگر آموزش یک شبکه عصبی تبدیل به یک مسئله بهینه سازی می‌شود و برای حل آن بسیاری از روش‌های بهینه سازی هوشمند آزمایش شده‌اند. به طور نمونه الگوریتم ژنتیک [15] [۸]، الگوریتم جستجوی گرانشی[16] [۸]، بهینه سازی ازدحام ذرات [17] [۲۲] و تکامل تفاضلی[18] [۱۹] برای آموزش شبکه‌های عصبی در حوزه تشخیص نفوذ مورد استفاده قرار گرفته‌اند.

در این تحقیق از الگوریتم رقابت استعماری[19] برای آموزش شبکه عصبی پرسپترون چند لایه استفاده شده است، تا با حل مسئله بهینه سازی آن بهترین وزن‌ها و بایاس‌ها برای شبکه انتخاب شده و دقت شبکه را در تشخیص نفوذ افزایش دهد.

ساختار این مقاله به این صورت است که در بخش ۲ کلیاتی از تحقیق شامل دو زیر بخش شبکه

[9] Artificial Intelligence (AI)
[10] Multi-Layer Perceptron (MLP)
[11] Radial Based Function (RBF)
[12] Support Vector Machine (SVM)
[13] Decision Tree (DT)
[14] Gradient Descend (GD)
[15] Genetic Algorithm (GA)
[16] Gravitational Search Algorithm (GSA)
[17] Particle Swarm Optimization (PSO)
[18] Deferential Evolution (DE)
[19] Imperialist Competitive Algorithm (ICA)

عصبی پرسپترون چند لایه و الگوریتم رقابت استعماری مرور می‌شوند. در بخش ۳ روش پیشنهادی مطرح شده و در بخش۴ نتایج ارائه شده و در انتها نتیجه‌گیری آمده است.

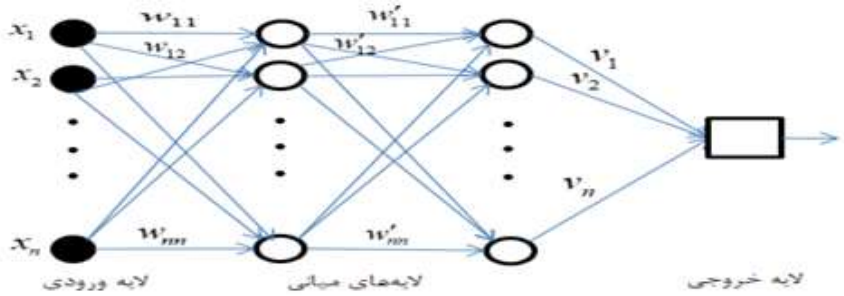
۲ کلیات تحقیق

۱.۲ شبکه‌های عصبی پرسپترون چند لایه (MLP)

MLP یک از انواع شبکه‌های عصبی است که در بسیاری از مسائلی که راه‌حل‌های کلاسیک آن‌ها با خطاهای زیادی همراه است پاسخ‌های قابل قبولی ارائه می‌کند و بنابراین یکی از شبکه‌های عصبی بسیار پرکاربرد است. معماری این شبکه به صورت پیش‌خور بوده و اغلب از روش‌های مبتنی بر کاهش شیب (GD) برای آموزش آن استفاده می‌شود. معماری پیش‌خور[۲۰] MLP در حالت کلی دارای سه واحد ورودی، میانی و خروجی است. واحد ورودی که ورودی‌های مسئله به آن اعمال می‌شود بر اساس مسئله تعریف خواهد شد به‌طوری که تعداد نرون‌های آن به تعداد ورودی‌های مسئله بستگی دارد. به همین صورت واحد خروجی هم مطابق با خروجی مسئله تنظیم شده و تعداد نرون‌های آن مساوی با تعداد خروجی‌های مسئله است. اما تعداد نرون‌های واحد میانی یکی از پارامترهای آزاد MLP است که باید تنظیم شود. واحدهای MLP با یک سری پارامتر به هم متصل می‌شوند که وزن نامیده می‌شوند، همچنین هر واحد ورودی مجزایی به نام پارامتر بایاس دارند تنظیم این دو پارامتر فرآیند آموزش شبکه عصبی را تشکیل می‌دهد. توابع انتقال [۲۱] یکی دیگر از پارامترهای یک شبکه عصبی است که در انتهای هر واحد حاصل‌ضرب بردارهای ورودی، وزن‌ها و بایاس‌ها را به واحد بعدی نگاشت می‌دهد. با تعیین همه این پارامترها پیکربندی یک شبکه عصبی MLP به پایان رسیده و فقط فرآیند آموزش شبکه باقی می‌ماند. در شکل ۱ تصویری از یک MLP ارائه شده که در آن وزن‌های هر لایه (واحد) و بردار ورودی مشخص شده است [۱۴].

[20] Feed forward

[21] Transfer function



شکل ۱: شبکه عصبی MLP
[۱۴]

۲.۲ الگوریتم رقابت استعماری (ICA)

الگوریتم رقابت استعماری ICA یکی از الگوریتم‌های بهینه سازی مبتنی بر جمعیت است که از رفتار سیاسی اجتماعی انسان‌ها در جوامع مختلف الهام گرفته شده است. ذرات مورد استفاده در ICA کشور نام دارند و معادل کروموزم در GA و یا ذره در PSO عمل کرده و جواب‌های مسئله را نام کشور کد می‌کند. ICA برای حل یک مسئله بهینه‌سازی به طول n به طور تصادفی کشورهایی با همین طول به عنوان جواب اولیه تشکیل می‌دهد. این جواب‌ها امپراطوری اولیه را تشکیل می‌دهند. پس از این مطابق همه الگوریتم‌های تکاملی میزان شایستگی هر کشور براساس تابع شایستگی سنجیده شده و کشورهای با عملکرد بهتر به عنوان استعمارگر و بقیه به عنوان مستعمره دسته‌بندی می‌شوند. فرآیند جستجوی ICA شروع شده و هر استعمارگر سعی دارد مستعمراتش را به سوی خود جذب کرده و آن‌ها را به خود شبیه‌تر کند، که به سیاست همگون سازی[۲۲] شهرت دارد. اتفاقی که در ادامه در ICA رخ می‌دهد رقابت استعماری است که در آن هر استعمارگر بر سر جذب مستعمرات سایرین با هم رقابت می‌کنند. در طی این مرحله استعمارگر ضعیف کم‌کم تمامی مستعمراتش را از دست داده و در انتها خودش هم جذب یک استعمارگر خواهد شد. ICA تا جایی تکرار می‌شود که تنها یک امپراطوری باقی بماند که راه حل بهینه

[22] Assimilation

مسئله خواهد بود. این الگوریتم در هر مرحله با اجرای فرآیند انقلاب[۲۳] که در آن یک کشور به طور تصادفی تغییر خواهد داشت سعی می‌کند از افتادن در دام بهینه‌های محلی اجتناب کند [۴].

۳ روش پیشنهادی

در این بخش روش پیشنهادی مطرح می‌شود، که در آن از ICA برای آموزش MLP استفاده خواهد شد تا مدل پیشنهادی به عنوان یک IDS مورد ارزیابی قرار گیرد که داده‌های آموزش و آزمایش به صورت تصادفی انتخاب شده‌اند و مراحل این روش به صورت زیر است.

۱. تقسیم داده‌های ورودی به دو دسته آموزش و آزمایش، طراحی یک MLP خام مطابق ورودی‌ها و خروجی‌های مسئله و تحویل داده‌های آموزش به شبکه خام.

۲. فراخوانی ICA جهت آموزش MLP تشکیل شده در مرحله اول.

۳. تشکیل امپراطوری اولیه مطابق پارامترهای مجهولMLP.

۴. ارزیابی شایستگی امپراطوری‌های اولیه و تعیین استعمارگران و مستعمرات.

۵. شروع فرآیند جستجو که شامل رقابت استعماری و انقلاب است. این مرحله تا رسیدن به معیار توقف تکرار می‌شود. اگر الگوریتم به یکی از معیارهای توقف رسید وارد مرحله بعد شده در غیر این صورت فرآیند بهینه سازی مجدد تکرار می‌شود.

۶. داده‌های آزمایش به MLP آموزش دیده تحویل شده تا کارایی آن ارزیابی شود.

۴ ارزیابی نتایج

در این بخش، روش پیشنهادی مطرح شده در قسمت قبل مورد ارزیابی قرار می‌گیرد. برای این‌کار از پایگاه داده $KDDcup$۹۹ استفاده کرده و نتایج روش پیشنهادی را با دو الگوریتم مبتنی بر

[23] Revolution

کاهش شیب مقایسه می‌کنیم. این پایگاه داده شامل دو رفتار عادی[۲۴] (NRL) و حمله است، که حمله خود شامل چهار دسته انکار سرویس[۲۵] (DoS)، دسترسی از راه دور[۲۶] $(R2L)$،کاربر به عنوان ریشه[۲۷] $(U2R)$ وکاوش[۲۸] (PRB) است. هر نمونه شامل ۴۱ ویژگی است که ۳۴ تای آن عددی و مابقی نمادین هستند [۹]. از ICA برای آموزش MLP استفاده خواهد شد تا مدل پیشنهادی به عنوان یک IDS مورد ارزیابی قرار گیرد. معماری MLP یک معماری سه لایه با ۲۰ نرون در لایه میانی و توابع انتقال سیگموییید و خطی برای لایه‌های میانی و خروجی است. تعداد تکرارها در فرآیند آموزش برابر با ۵۰۰ و در ICA تعداد کشورها برابر ۱۰۰، تعداد امپراطوری اولیه ۳۰ و نرخ انقلاب و همانند سازی به ترتیب ۰٫۳ و ۰٫۵ در نظر گرفته شده است. معیارهای ارزیابی به ترتیب دقت[۲۹] و صحت[۳۰] هستند که در معادلات ۱ و ۲ نشان داده شده‌اند که پارامترهای آن به این صورت تعریف می شوند؛ مثبت صحیح $(TruePositive)$ حمله صورت گرفته به درستی حمله تشخیص داده شود، مثبت کاذب $(FalsePositive)$ حمله صورت گرفته به اشتباه عدم حمله تشخیص داده شود، منفی صحیح$(TrueNegative)$ حمله صورت نگرفته به درستی عدم حمله تشخیص داده شود و منفی کاذب$(FalseNegative)$ حمله صورت نگرفته به اشتباه حمله تشخیص داده شود. در انتها لازم به ذکر است تمامی پارامترهای آزاد الگوریتم رقابت استعماری و شبکه عصبی پرسپترون چند لایه با سعی و خطا تعیین شده‌اند.

$$accurracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (۱)$$

$$precision = \frac{TP}{TP + FP} \quad (۲)$$

[24] Normal
[25] Denial of service
[26] Remote to local
[27] User to root
[28] Probe
[29] Accuracy
[30] Precision

جدول ۱: مقادیر دقت

Accuracy	DoS	NRL	PRB	R۲L	U۲R
GD	۷۶٫۵	۶۸	۹۶٫۵	۸۴٫۲	۵۰
GDM	۷۷٫۵	۷۳٫۴	۷۷	۷۸	۵۰
MLP by ICA	۹۵	۷۸	۶۹	۴۵	۵۰

جدول ۲: مقادیر صحت

Precision	DoS	NRL	PRB	R۲L	U۲R
GD	۸۱	۴۸	۹۶	۷۱	N/A
GDM	۸۳	۵۴	۶۴	۶۳	N/A
MLP by ICA	۹۰	۵۸	۵۱	N/A	N/A

برای آموزش MLP از روش‌های مبتنی بر کاهش شیب از دو الگوریتم کاهش شیب (GD) و کاهش شیب با ممنتم (GDM) استفاده شده است. مقادیر دقت و صحت بر حسب درصد برای این دو الگوریتم و روش پیشنهادی به ترتیب در جداول ۱ و ۲ نشان داده شده‌اند.

همان‌طور که در جداول ۱ و ۲مشخص است روش پیشنهادی در تشخیص حمله DoS و عدم حمله به مراتب از دو روش دیگر عملکرد بهتری داشته است. همچنین روش پیشنهادی در دو حمله PRB و $R۲L$ از روش‌های مبتنی بر کاهش شیب عقب افتاده است. دلیل عملکرد بهتر روش پیشنهادی فرار از افتادن در دام بهینه‌های محلی است و دلیل کارایی پایین تر در دو حمله دیگر به تعداد کم نمونه‌های این حملات و عدم زمان کافی برای تکمیل فرآیند آموزش الگوریتم رقابت استعماری برمی‌گردد. در این مقاله از دو روش مشهور GD و GDM در مقایسه با روش پیشنهادی استفاده شده است، لازم به ذکر است که روش‌های مبتنی بر گرادیان در مرحله اجرا هزینه محاسباتی پایینی داشته و از این نظر نسبت به روش پیشنهادی برتری دارند. در کاربردهای مختلف بین هزینه محاسباتی و دقت کار یک توازن برقرار شده و در سیستم‌های تشخیص نفوذ بیشتر دقت پیش بینی ارجحیت داشته و بنابراین با صرف یک هزینه محاسباتی نتایج بهتری حاصل خواهد شد.

۵ نتیجه گیری

درسال‌های اخیر حملات به شبکه‌های کامپیوتری بسیار افزایش یافته و به مراتب مقابله با آن‌ها هم پیچیده‌تر شده است. تشخیص نفوذ یکی از زمینه‌های تحقیقاتی است که برای کمک به امنیت شبکه‌های کامپیوتری استفاده می‌شود. در این مقاله سعی شد تا با آموزش شبکه عصبی پرسپترون چند لایه با الگوریتم رقابت استعماری بهبودی در تشخیص نفوذ بر روی پایگاه داده KDD ایجاد شود. خوشبختانه روش پیشنهادی با دوری از بهینه‌های محلی و آموزش بهتر به نتایج قابل توجهی رسید.

مراجع

[1] M. S. Abadeh, H. Mohamadi and J. Habibi, Design and analysis of genetic fuzzy systems for intrusion detection in computer networks, Expert Syst. Appl., 38 (2011), 7067-7075.

[2] B. Agarwal and N. Mittal, Hybrid approach for detection of anomaly network traffic using data mining techniques, Proceedings of ICCCS, (2012), Procedia Technology, 6 (2012), 996-1003.

[3] R. Ashok, A. Lakshmi, G. V. Rani and M. N. Kumar, Optimized feature selection with k–means clustered triangle SVM for intrusion detection, Proceedings of ICoAC, (2011), 23-27.

[4] E. Atashpaz-Gargari and C. Lucas, Imperialist Competitive algorithm: An algorithm for optimization inspired by imperialist competition, Proceedings of the CEC, (2007), 4661-4667.

[5] A. A. Aziz, S. E. Hanafi and A. E. Hassanien, Comparison of classification techniques applied for network intrusion detection and classification, J. Appl. Logic, 24 (2017), 109–118.

[6] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, Network anomaly detection: methods, systems and tools, IEEE Commun. Surv. Tutor., 16(1) (2014), 303-336.

[7] E. Corchado and A. Herrero, Neural visualization of network traffic data for intrusion detection, Appl. Soft. Comput., 11 (2011), 2042-2056.

[8] T. Dash, A Study on Intrusion Detection Using Neural Networks Trained with Evolutionary Algorithms, soft comput., 21(10), (2017), 2687-2700.

[9] S. Devaraju and S. Ramakrishnan, Detection of accuracy for intrusion detection system using neural network classifier, Int. J. Emerging Technol. Adv. Eng., 3 (2013), 2250-2459.

[10] R. Devi, R. K. Jha, A. Gupta, S. Jain and P. Kumar, Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network, INT. J. ELECTRON. C., 74(2017), 94-106.

[11] W. Feng, Q. Zhang, G. Hu and J. X. Huang, Mining network data for intrusion detection through combining SVMs with ant colony networks, Future Gener. Comput. Syst., 37 (2014), 127–140.

[12] F. Haddadi, S. khanchi, M. Shetabi and V. Derhami, Intrusion detection and attack classification using feed-forward neural network, Proceedings of ICCNT, (2010), 262-266.

[13] R. G. Helali, Data mining based network intrusion detection system: A survey, in: Novel Algorithms and Techniques in Telecommunications and Networking, Springer Science+Business, (2010).

[14] M. Kuchaki Rafsanjani and M. Samareh, Chaotic time series prediction by artificial neural networks, J. Comput. Meth. Sci. Eng., 16 (2016), 599-615.

[15] M. Kuchaki Rafsanjani and Z. A. Varzaneh, Intrusion detection by data mining algorithms: a review, J. New Resul. Sci., 2 (2013), 76-91.

[16] S. A. Mulay, P. R. Devale and G. V. Garje, Decision tree based support vector machine for intrusion detection, Proceedings of ICNIT, (2010), 59-63.

[17] S. Pilabutr, P. Somwang and S. Srinoy, Integrated soft computing for intrusion detection on computer network security, Proceedings of ICCAIE, (2011), 559-563.

[18] A. Rapaka, A. Novokhodko and D. Wunsch, Intrusion detection using radial basis function network on sequence of system calls, Proceedings of IJCNN03, (2003), 1820-1825.

[19] Z. Salek, F. M. Madani R. azmi, Intrusion detection using Neural Networks trained by differential evaluation algorithm, Proceedings of ISCISC , (2013).

[20] P. Sangkatsanee, N. Wattanapongsakorn and C. Charnsripinyo, Practical real-time intrusion detection using machine learning approaches, Comput. Commun., 34 (2011), 2227-2235.

[21] S. S. Sivatha Sindhu, S. Geetha and A. Kannan, Decision tree based light weight intrusion detection using a wrapper approach, Expert Systems with Applications, 39 (2012), 129-141.

[22] W. J. Tian and J. C. Liu, Network intrusion detection analysis with neural network and particle swarm optimization algorithm, Proceedings of the CCDC, (2010), 1749-1752.

[23] G. Wang, J. Hao, J. Ma and L. Huang, A New approach to intrusion detection using artificial neural networks and fuzzy clustering, Expert Syst. Appl., 37 (2010), 6225-6232.

[24] Sh. X. Wu and W. Banzhaf, The use of computational intelligence in intrusion detection systems: a review, Appl. Soft Comput., 10 (2010), 1-35.

[25] C. Zhang, J. Jiang and M. Kamel, Intrusion detection using hierarchical neural networks, Pattern Recognit. Lett., 26 (2005), 779-791