



تشخیص نفوذ در شبکه‌های حسگر بی‌سیم با استفاده از روش طبقه‌بندی Naive Bayesian

مؤلف:

سیده الهه مرتضوی اصل

(کارشناسی ارشد مهندسی کامپیوتر - نمره ممتاز)

دکتر همایون ابراهیمیان

(عضو هیات علمی دانشگاه آزاد اسلامی واحد اردبیل)

سرشناسه: مرتضوی اصل، سیده‌الیه، ۱۳۶۱ -
 عنوان و نام پدیدآور: تشخیص نفوذ در شبکه‌های حسگر بی‌سیم با استفاده از روش
 طبقه‌بندی Naive Bayesian/ مولفین سیده‌الیه مرتضوی اصل، همایون ابراهیمیان.
 مشخصات نشر: اردبیل: گونش نگار، ۱۳۹۶.
 مشخصات ظاهری: ۱۰۵ ص.
 شابک: ۱۳۰۰۰۰ ریال ۶-۶-۹۷۷۲۷-۶۰۰-۹۷۸:
 وضعیت فهرست نویسی: فیپا
 یادداشت: کتابنامه
 موضوع: شبکه‌های حسگر بی‌سیم
 موضوع: Wireless sensor networks
 موضوع: شبکه‌های حسگر بی‌سیم -- تدابیر ایمنی
 موضوع: Wireless sensor networks -- Security measures
 موضوع: شبکه‌های حسگر بی‌سیم -- الگوهای ریاضی
 موضوع: Wireless sensor networks -- Mathematical models
 شناسه افزوده: ابراهیمیان، همایون، ۱۳۵۱ -
 رده بندی کنگره: ۸۷۲TK، نشر ۱۳۹۶، ۴۴
 رده بندی دیویی: ۸۲۲/۰۰۴
 شماره کتابشناسی ملی: ۱۱۹۷۶۷۰

◀ نام کتاب : تشخیص نفوذ در شبکه‌های حسگر بی‌سیم با استفاده از روش

طبقه‌بندی Naive Bayesian

◀ مؤلفین : سیده‌الیه مرتضوی اصل و همایون ابراهیمیان

◀ ناشر : انتشارات گونش نگار

◀ نوبت چاپ : اول ۹۶

◀ تیراژ : ۱۱۰۰ جلد

◀ قیمت : ۱۳۰۰۰۰ ریال

◀ شابک : ۹۷۸-۶۰۰-۹۷۷۲۷-۶۰۰-۹۷۸



آدرس: اردبیل، اول خیابان دانشگاه، روبروی اداره مخابرات، انتشارات گونش نگار

۰۴۵-۳۳۵۲۳۳۵۹

mail.xepersian.print@yahoo.com

همه حقوق چاپ و نشر برای مولفین محفوظ است.

فهرست مطالب

عنوان	صفحه
پیشگفتار	۱۱
فصل اول - روشهای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم	۱۳
۱-۱- مقدمه	۱۴
۱-۲- خطرهای حملات امنیتی	۱۵
۱-۳- تشخیص نفوذ در شبکه‌های ad-hoc: فرمول بازی بیزی	۱۷
۱-۴- سیستم تشخیص نفوذ با استفاده از بررسی پروفایل ترافیک شبکه و ماشین یادگیری ترتیبی آدریز	۱۹
۱-۵- روش ترکیبی سیستم‌های فازی ژنتیک و یادگیری دو به دو برای بهبود نرخ تشخیص در سیستم‌های تشخیص نفوذ	۲۲
۱-۶- روش پیشنهادی: سیستم‌های فازی ژنتیک و یادگیری دو به دو	۲۲
۱-۷- سیستم‌های فازی ژنتیک، الگوریتم FARC-HD	۲۳
۱-۸- طبقه‌بندی از طریق تکنیک‌های ساجا: یک در مقابل یک	۲۴
۱-۹- مزایای هم‌افزایی GFS و OVO برای IDS	۲۵
۱-۱۰- طبقه‌بندی کارآمد با استفاده از مدل مواری و مدل فشرده مقیاس پذیر و استفاده از آن در تشخیص نفوذ	۲۷
۱-۱۱- فشرده سازی مدل موازی و مقیاس پذیری داده‌های آماری	۲۸
۱-۱۱-۱- نرمال سازی داده‌ها	۲۸
۱-۱۱-۲- فشرده‌گی افقی	۲۸
۱-۱۱-۳- فشرده سازی عمودی	۲۹
۱-۱۱-۴- توصیف مختصر روش پیشنهادی	۲۹
۱-۱۱-۵- تکامل مجموعه قانون آماری برای تشخیص نفوذ شبکه	۳۱
۱-۱۱-۶- رویکرد مبتنی بر GA پیشنهادی	۳۲
۱-۱۱-۷- بازنمود انفرادی	۳۴
۱-۱۲- بهبود عملکرد سیستم تشخیص نفوذ شبکه از طریق کیفیت پیکربندی سرویس و تکنولوژی موازی	۳۷
۱-۱۳- روش جدید SVM-KNN-PSO برای سیستم‌های تشخیص نفوذ	۳۸
۱-۱۳-۱- طبقه‌بند KNN	۴۰

۴۰	۱-۱۳-۲- رویکرد گروهی با WMV
۴۴	۱-۱۳-۳- الگوریتم اکثریت وزن
۴۵	۱-۱۴- یک سیستم تشخیص نفوذ براساس ترکیب مراکز خوشه و نزدیکترین همسایه CANN
۴۸	۱-۱۴-۱- تشکیل داده‌های جدید
۴۸	۱-۱۵- چارچوب مشترک برای تشخیص نفوذ در شبکه‌های سیار
۵۰	۱-۱۶- طراحی دو لایه سیستم تشخیص نفوذ شبکه
۵۲	۱-۱۷- مقایسه روش‌های تشخیص نفوذ
۵۵	فصل دوم - طبقه بندی Naive Bayesian
۵۶	۱-۲- مقدمه
۵۷	۱-۲-۱- روش طبقه بندی Naive Bayes
۵۹	۳-۲- تعریف الگوریتم
۶۴	۲-۴- قدرت علی رغ استقلال
۶۶	۲-۵- گستردگی داده‌ای مدل
۷۱	۲-۶- روش پیشنهادی
۷۳	۲-۷- انتخاب زیرمجموعه ویژگی
۷۹	فصل سوم - پیاده سازی طبقه بندی Naive Bayesian
۸۰	۳-۱- مقدمه
۸۰	۳-۲- پیاده سازی روش پیشنهادی
۸۷	۳-۳- پیش پردازش داده‌ها
۸۸	۳-۴- انتخاب زیر مجموعه ویژگی‌ها
۸۹	۳-۵- نرمالسازی داده‌ها
۸۹	۳-۶- پیاده سازی مدل طبقه بندی Naive Bayesian
۹۵	فصل چهارم - ارزیابی عملکرد طبقه بندی Naive Bayesian
۹۶	۴-۱- ارزیابی عملکرد روش پیشنهادی
۱۰۰	۴-۲- مقایسه روش پیشنهادی با روش‌های پیشین
۱۰۲	۴-۳- نتیجه گیری
۱۰۴	مراجع

فهرست جداول

عنوان	صفحه
جدول ۱-۱: تعداد مشاهدات در مجموعه داده KDD99 [11]	۳۹
جدول ۲-۱: الگوریتم تشخیص نفوذ دوسطحی	۵۱
جدول ۳-۱: مزایا و معایب روش‌های تشخیص نفوذ در شبکه	۵۳
جدول ۱-۲: الگوریتم طبقه‌بندی Naive Bayesian	۷۷
جدول ۱-۳: ویژگی‌های پایه اتصالات تکی tcp	۸۴
جدول ۲-۳: ویژگی‌های محتوایی با اتصالات پیشنهادی توسط دامنه دانش	۸۴
جدول ۳-۳: ویژگی‌های ترافیک محاسبه شده با استفاده از پنجره زمانی دو ثانیه ای	۸۵
جدول ۴-۳: ویژگی‌های محاسبه شده برای میزبان مقصد در پنجره دو ثانیه ای	۸۵
جدول ۵-۳: نمونه ای از اتصالات موجود در میان داده‌ها	۸۶
جدول ۶-۳: توزیع نمونه های آموزشی در کلاس ها	۹۰
جدول ۷-۳: توزیع احتمال تغییراتی های غیر عددی	۹۱
جدول ۷-۳: محاسبه احتمال توزیع بد معیار خاص از ویژگی src_bytes	۹۲
جدول ۳-۴: دقت روش پیشنهادی طی مراحل افزایش نمونه‌های تست	۹۹

فهرست شکل‌ها

عنوان	صفحه
شکل ۱-۱: فلوچارت سیستم تشخیص نفوذ با استفاده از بررسی پروفایل	۲۰
شکل ۲-۱: مراحل ساخت الگوریتم FARC-HD	۲۵
شکل ۳-۱: چارچوب کلی روش فشرده سازی و توزیع مجموعه داده آموزشی	۲۹
شکل ۴-۱: معماری سیستم پیشنهادی مبتنی بر الگوریتم ژنتیک	۳۳
شکل ۵-۱: ساختار سیستم کروموزوم	۳۴
شکل ۶-۱: ساختار طبقه‌بند KNN	۴۰
شکل ۷-۱: اختار الگوریتم فرا بهینه سازی برای PSO	۴۳
شکل ۸-۱: مراحل CANN	۴۷
شکل ۱-۲: چارچوب روش پیشنهادی	۷۸
جدول ۸-۳: مثال‌هایی از نتایج تشخیص نمونه‌های تست به کلاس با احتمال بیشتر	۹۳
شکل ۱-۴: تعداد خطاهای موجود در بیان گزارش‌های اتصال تست	۹۷
شکل ۲-۴: گزارش‌های اتصال تست با نتیجه ندری صحیح	۹۸
شکل ۵-۴: دقت روش پیشنهادی	۱۰۰
شکل ۶-۴: مقایسه روش پیشنهادی با روش‌های پیشین	۱۰۱

پیشگفتار

با توجه به گستردگی استفاده از شبکه‌های ارتباطی و در رأس آن‌ها اینترنت و همچنین سهولت برقراری ارتباط از طریق شبکه‌های بی‌سیم، این نوع از شبکه‌ها بیش از پیش مورد توجه قرار گرفته‌اند. قابلیت استفاده در هر محیط و بدون نیاز زیر ساخت و ارتباطات فیزیکی همچنین عدم نیاز به نظارت و مهندسی محیط که از مشخصه‌های منحصر به فرد این شبکه‌هاست، باعث کاربرد روزافزون شبکه‌های بی‌سیم در زمینه‌های مختلف شده است. شبکه‌های حسگر بی‌سیم زیر مجموعه‌ای از شبکه‌های بی‌سیم است که به منظور جمع‌آوری اطلاعات از محیط اطراف به وجود آمده‌اند. این شبکه‌ها از حسگرهایی تشکیل شده‌اند که در سرتاسر محیط مورد نظر پراکنده شده و داده‌های مربوط به حوادث رخ داده در این محیط را برای بررسی و اقدامات لازم گزارش می‌کنند. گره‌های حسگر بی‌سیم برای برقراری ارتباط با همدیگر و با حفرة که موظف به جمع‌آوری اطلاعات از حسگرهاست از مایای گره‌های بی‌سیم بهره می‌برند به همین دلیل مورد توجه کاربردهای بسیاری قرار یافته‌اند. از سوی دیگر افزایش کاربرد آن‌ها باعث مطرح شدن چالش‌های زیادی در زمینه ارسال و دریافت اطلاعات شده که امنیت به عنوان مهم‌ترین مسئله مطرح شده است. این شبکه‌ها به دلیل بی‌سیم بودن، محدودیت منابع، تحرک و پویایی و وظایف مهم و بحرانی که دارند نسبت به شبکه‌های دیگر دارای آسیب‌پذیری نسبتاً بالایی هستند.

برای ایجاد امنیت در شبکه‌های بی‌سیم روش‌های مختلفی پیشنهاد شده است ولی این روش‌ها قادر به تشخیص اکثر حملات نیستند. نفوذ گره‌های مخرب در میان گره‌های این شبکه می‌تواند موجب تضعیف و یا تخریب بسته‌های اطلاعاتی انتقال یافته شود و تمام یا قسمتی از اطلاعات مورد نیاز از بین برود. در نتیجه کارایی کل سیستم تهدید شده و ممکن است نتایج به گونه دیگری مورد تفسیر قرار گیرند. بنابراین جلوگیری و کشف نفوذها و حملات در شبکه‌های حسگر بی‌سیم به یک امر حیاتی و

چالشی جدی تبدیل شده است. از این رو سیستم‌های تشخیص نفوذ نقش مهمی در ایجاد امنیت در شبکه‌های بی‌سیم بر عهده دارند و می‌توانند محدوده وسیعی از حملات را در برگیرند.

از سوی دیگر با توجه به انرژی محدود گره‌های حسگر بی‌سیم، استفاده از گره‌های ناظر برای نظارت دائمی در شبکه‌های حسگر بی‌سیم به منظور جلوگیری و کشف نفوذ و حملات را در این نوع از شبکه‌ها عملاً غیر ممکن کرده است. به عنوان راه حلی برای غلبه بر این مشکل، امروزه بحث سیستم‌های کنترلی و نظارت از راه دور به یکی از مباحث مورد علاقه در زمینه‌های مختلف تبدیل شده است. نظارت از راه دور بر عملکرد و رفتار گره‌ها، وجود در شبکه‌های حسگر بی‌سیم علاوه بر تشخیص گره‌های مخرب و بد رفتار درون شبکه می‌تواند به پیش بینی رفتار گره‌های بد رفتار در آینده نیز بیانجامد. بالطبع با تشخیص دهی بد رفتار، از ایجاد نفوذ و حملات در شبکه که می‌تواند خطری برای اطلاعات اسفال یافته در شبکه به حساب آید، جلوگیری به عمل می‌آید. علاوه بر این نظارت از راه دور موجب کاهش انرژی مصرفی در گره‌های حسگر بی‌سیم شده و از لحاظ هزینه نیز مقرون به صرفه تر خواهد بود.