الملخص

مع التزايد العالي لسرعة شبكات الحاسوب اليوم ، التي تؤثر بشكل مباشر على أداء وسائل الحماية من حيث سرعة الكشف، فإن أدوات الحماية التقليدية مثل الجدار الناري غير كافية لتوفير شبكات متكاملة ، موثوق بها و آمنة.

نظام كشف التسلل(IDS) هو أحد الأدوات الأكثر موثوقية الذي يمكن استخدامه لمراقبة حركة مرور الشبكة الداخلة و الخارجة لتحديد الإستخدام غير المصرح به و سوء معالجة شبكات نظام الحاسوب.

يرجع ذلك إلى حقيقة، البرمجيات التي تستخدم نظام كشف التسلل في الشبكة لا تزال غير قادرة على كشف جميع التهديدات المتزايدة في رابط عالي السرعة. المهمة الرئيسية لهذا النوع من الهجمات هي لتوليد كمية كبيرة من حركة المرور بسرعة عالية للرابط الذي يؤدي إلى إبطاء أداء محرك الكشف في NIDS.

في هذه الدراسة، اقترحنا قابلة خوارزمية مطابقة الجمل المرنة بالاعتماد على NIDS لتعزيز سرعة محرك الكشف في NIDS التي سميت خوارزمية مطابقة الجمل المرنة متعددة المعالجة لنظام كشف التسلل في الشبكة (MSNIDS). MSNIDS نفذت باستخدام خوارزمية المطابقة الدقيقة الموزونة المحسنة(EWEMA) في كلا السيناريوهين في المعالجة المتسلسلة والمتوازية.

ووجد أن سرعة محرك الكشف يمكن أن تتحسن في كل من المعاجة المتسلسلة و المتوازية عبر تحسين خوارزمية المطابقة الدقيقة الموزونة و تسمى(EWEMA). تحسينات المعالجة المتسلسلة لEWEMA خفضت عدد المقارنات المطلوبة لمطابقة محتوى كل حزمة واردة مع مجموعات القواعد. وبالإضافة إلى ذلك، فإن المعالجة المتوازية التي تستخدم المعالجات المتعددة المختلطة مع تقنية النوى المتعددة كما أنها زادت سرعة محرك الكشف لجعل NIDS يعمل مع رابط عالي السرعة بكفاءة.

ويستنتج من ذلك أن، خوارزمية مطابقة الجمل المرنة متعددة المعالجة لنظام كشف التسلل في الشبكة بالاعتماد على خوارزمية المطابقة الدقيقة الموزونة المحسنة يمكن أن تحقق أكثر من 89٪ من وقت المعالجة المتسلسلة مقارنة مع خوارزمية المطابقة الدقيقة الموزونة ، و 86٪ من وقت المعالجة المتوازية مقارنة مع المعالجة المطابقة المتسلسلة.