عنوان مقاله:
الگوریتم جدیدی از هش با استفاده از شبکه عصبی آشوبگر، قابل استفاده در پرو تکل های امنیتی تبادلی

محل انتشار:
اولین کنفرانس ملی مهندسی برق اصفهان (سال: 1391)

تعداد صفحات اصل مقاله: 9

نویسندگان:
سمیرا اصغری اباتری - *دانشجوی کارشناسی ارشد مخابرات سیستم دانشگاه آزاد اسلامی واحد تهران جنوب*

منصور نجاتی جهرمی - *استادیار گروه مخابرات دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد تهران جنوب*

احمد علمایی - *استادیار گروه مخابرات دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد تهران جنوب*

خلاصه مقاله:
در این مقاله یک الگوریتم برای ساخت تا به هش بر اساس ساختار شبکه عصبی آشوبگر CNN دو لایه پیشنهاد شده است که می‌تواند در پرو تکلهای امنیتی تبادل این مثل Ipsec در شبکه‌های مخابراتی مورد استفاده قرار گیرد. همچنین ما از یک تابع تبدیل تکه ای خطی PWLCM به عنوان تابع انتقال استفاده کرده‌ایم که قابلیت آشوب را در شبکه عصبی فراهم می‌کند و نیز در این مقاله یک تابع چهار بعذی 4D-OWCML به عنوان تولیدکننده شبکه عصبی آشوب گر کار گرفته شده است. تجزیه و تحلیل نظری و شبیه سازی‌های صورت گرفته نشان می‌دهد که الگوریتم پیشنهاد شده دارای چندین خاصیت مانند تعداد پیام بالا و حساسیت کلید، خواص آماری مناسب و مقابله با حمله مرد میانی است که می‌تواند عملکرد مورد نیاز تابع هش را در شبکه مورد نظر برآورد کند.

کلمات کلیدی:
تابع هش ، شبکه عصبی آشوب گرد، رمز نگاری، تولید کلید، پروتکل امنیتی تعادلی، تابع تبدیل PWLCM

لینک ثابت مقاله در پایگاه سیویلیکا: