

عنوان مقاله:

مطالعه ای بر تکنیکهای بهینه سازی در هوش مصنوعی جهت حل مسئله ی SVP در تئوری شبکه ها

محل انتشار:

چهارمین کنفرانس ملی فناوری در مهندسی برق، کامپیوتر (سال: 1397)

تعداد صفحات اصل مقاله: 35

نویسندگان:

غلامرضا مغیثی - دانشکده ICT، دانشگاه صنعتی مالک اشتر تهران، تهران

علی پاینده - استادیار، دانشکده ICT، دانشگاه صنعتی مالک اشتر تهران، تهران

خلاصه مقاله:

بزرگترین چالش امنیتی پیشروی طرحها و پروتکل‌های رمزنگاری شبکه مینا، میزان سختی مسائل شبکه در ساختار این طرحهاست که یکی از مهمترین و پایه ای ترین آنها را میتوان مسئله SVP به شمار آورد. اگرچه روشهای موثر خاص منظوره‌های در تئوری شبکه جهت تقریب حل مسئله SVP وجود دارد ولی تکنیکهای عمومی دیگری نیز وجود دارد که این مسئله را به دیده ی یک جعبه ی سیاه نگریسته و اقدام به حل آنها مینماید (درحالیکه قابلیت بهره‌گیری از دانش فضای مسئله را در فرایند جستجوی خود مهیا میکند). در این پژوهش تلاش به بررسی فنی امکان بکارگیری مهمترین تکنیکهای هوش مصنوعی در کلاس جستجوهای تصادفی هدایت شده (از قبیل محاسبات تکاملی، روشهای مکانیک آماری، سیستمهای فازی، شبکه های عصبی و شبکه های عصبی فازی) جهت حمله به مسئله SVP نمودیم. بکارگیری الگوریتمهای تکاملی بیشترین درجه ی سازگاری در حمله به SVP نسبت به تکنیکهای دیگر نشان داده است. متأسفانه استفاده‌ی مستقیم از سیستمهای فازی و شبکه های عصبی فازی در طراحی حمله به SVP بسیار ناامید کننده بوده است (هرچند در این پژوهش، کاربردهای مناسبی برای بکارگیری این تکنیکها در حملات شبکه پیشنهاد شده است). همچنین، بررسی فنی بکارگیری تکنیکهای مکانیک آماری و شبکه های عصبی، ملاحظات و مشکلاتی را آشکار نمود که لحاظ آنها در مطالعات آتی میتواند مفید واقع شود.

کلمات کلیدی:

رمزنگاری مبتنی بر شبکه، مسئله ی SVP، سیستم های تکاملی، مکانیک آماری، الگوریتم متروپولیس، شبکه های عصبی، شبکه های عصبی فازی، سیستمهای فازی.

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/928959>

