عنوان مقاله:
ارایه یک الگوریتم کارا برای ساخت و پیمایش زنجیره های در هم ریز

محل انتشار:
دومین کنفرانس ملی دستاورهای نوین در برق وکامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
علیرضا محمدی ندوشن - *مربی، دانشکده فنی و مهندسی، دانشگاه ولی عصر (عج) رفسنجان*

عباس شاهمرادی - *فارغ التحصیل دانشکده برق و کامپیوتر، دانشگاه سمنان*

خلاصه مقاله:
از زمان معرفی توسط Lamport، زنجیره های یک طرفه تا کنون در کاربردهای امنیتی زیادی مورد استفاده قرار گرفته اند. با وجود کارایی زنجیره های یک طرفه تا کنون در کاربردهای امنیتی زیادی مورد استفاده قرار گرفته اند. با وجود کارایی زنجیره های یک طرفه، رتبه پیچیدگی حافظه ای محاسباتی ومحدودیت طول آن ها به عنوان دو دغدغه طراحان پروتکل های مبتنی بر این زنجیره ها مطرح هستند. الگوریتم های متنوعی برای حل هر یک یا هر دو این مشکلات تا کنون ارایه شده است. این مقاله یک الگوریتم جدید را برای حل این دو مشکل ارایه می کند. این الگوریتم نسبت به راه کارهای مشابه علاوه بر این که مشکل محدودیت طول را حل می کند سربار محاسباتی و ارتباطی پایین تری را تحمیل می کند علاوه بر این امنیت این الگوریتم نیز توسط شبیه سازی امنیتی AVISPA به صورت فرمال بررسی و اثبات شده است.

کلمات کلیدی:
زنجیره های یک طرفه، پیمایش زنجیره ها، رتبه پیچیدگی حافظه محاسبه ای